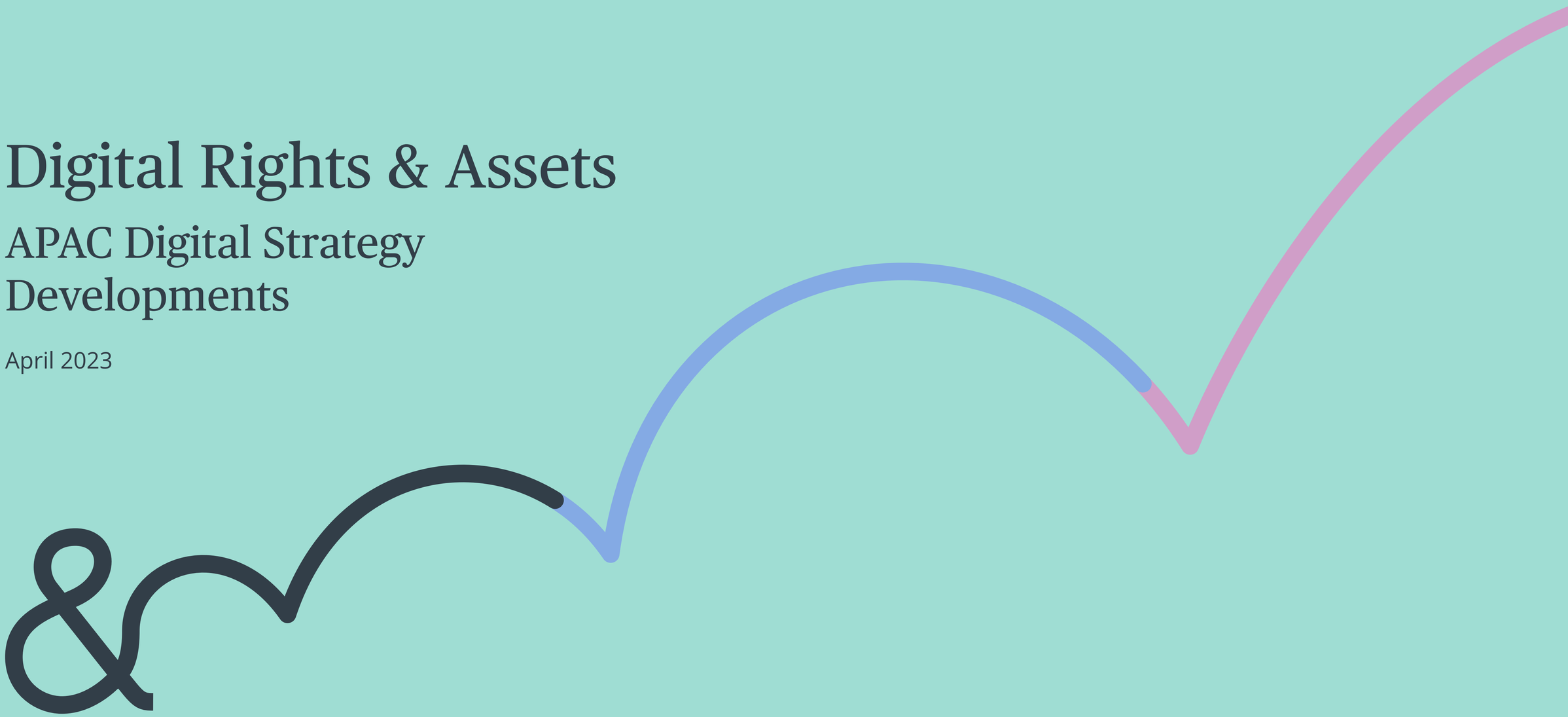
Bird & Bird

One firm.
Your firm.

Digital Rights & Assets

APAC Digital Strategy Developments

April 2023



Exploitation of digital rights & assets across the world is *vast and growing*

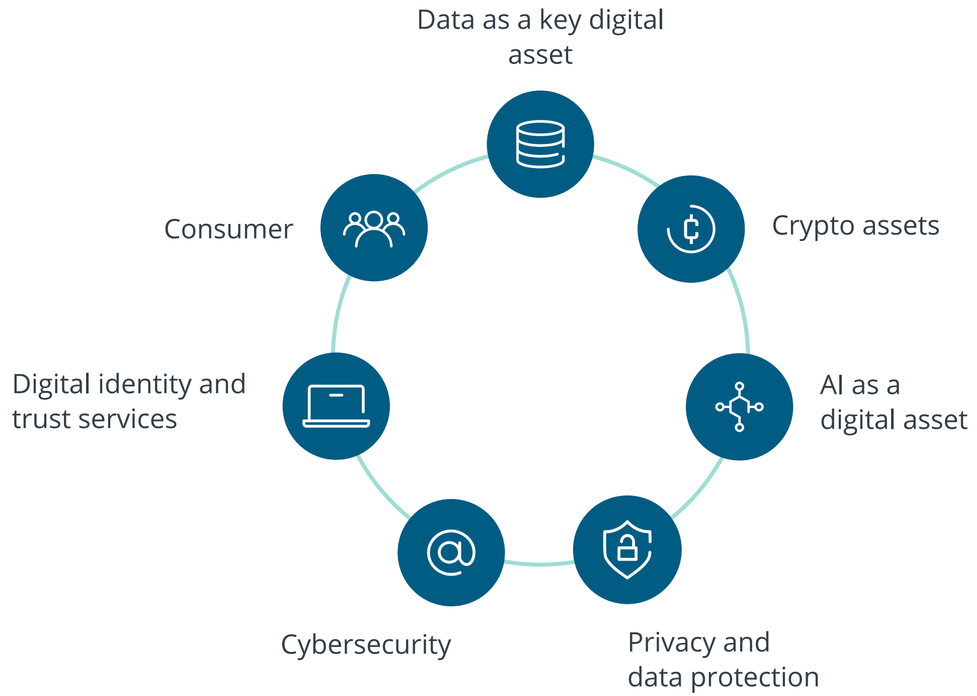
Data, content, currencies and online reputations are some of the most valuable parts of the asset base of many businesses worldwide. Digital assets are often essential to the effective understanding, management, operation and growth of organisations, and are at the forefront of organisations' thinking as they look ahead to a world of interconnected devices and ultrafast connectivity.

At a time of intensifying regulatory activity in the digital & tech sector, the APAC region is seeking to align itself with developments overseas, and effective digital asset management is commonly a core component of compliance. But with so many moving parts in this field, what do you need to be aware of?

This APAC digital regulatory strategy developments guide covers the latest developments, how they are relevant to your jurisdiction and what next steps you need follow.

We also have a European version of this publication, covering the latest developments involving data, crypto assets, AI as a digital assets, privacy and data protection, cyber security and digital identity and trust services, click **here** to access the guide.

Click on the icons below to navigate to the section you'd like to learn about.



Data as a key digital asset

CHAPTER 1

Australia

China

Singapore

Regulation of internet intermediaries & online platforms generally

Digital Advertising

Content Moderation

- Misinformation/Disinformation
- Harmful Content: Online Safety Act 2021 (Cth)
- Defamation: Social Media (Anti-Trolling) Bill 2022

Australia

Regulation of internet intermediaries & online platforms generally

Digital Advertising

Content Moderation

Misinformation/Disinformation

Harmful Content: Online Safety Act 2021 (Cth)

Defamation: Social Media (Anti-Trolling) Bill 2022

Latest developments:

The Australian Competition and Consumer Commission (**ACCC**) is currently undertaking a 5-year inquiry into digital platform services, examining:

- The intensity of competition in markets for the supply of digital platform services, with particular regard to the concentration of power, the behaviour of suppliers, mergers and acquisitions, barriers to entry or expansion and changes in the range of services offered by suppliers of digital platform services;
- Practices of suppliers in digital platform services markets which may result in consumer harm;
- Market trends that may affect the nature and characteristics of digital platform services; and
- Developments in markets for the supply of digital platform services outside Australia.

Interim reports released as part of this inquiry to date have covered:

- Competition and consumer issues associated with the distribution of mobile apps to users of smartphones and other mobile devices, focussing in particular on app marketplaces;
- Competition and consumer issues in relation to search and social media platforms and online private messaging services in Australia;
- Market dynamics and consumer choice screens in search services and web browsers; and
- Stronger consumer protections regarding certain digital platforms, including improved dispute resolution processes and an independent ombudsman.

How could it be relevant for you?

The ACCC's previous and similar inquiry, the Digital Platforms Inquiry (concluded in July 2019) (**Digital Platforms Report**) resulted in the extensive reform process currently underway in respect of the *Privacy Act 1988* (Cth) (**Privacy Act**) (referred to in chapter 4). It is expected that suppliers of digital platform services will be similarly affected by reforms arising out of the ACCC's eventual recommendations, although it is too early to determine what these may be.

Next steps:

The final report of the digital platform services inquiry is not due to be handed down until 31 March 2025.

Australia

Regulation of internet intermediaries & online platforms generally

Digital Advertising - 1/2

Content Moderation

Misinformation/Disinformation

Harmful Content: Online Safety Act 2021 (Cth)

Defamation: Social Media (Anti-Trolling) Bill 2022

Latest developments:

In September 2021, the ACCC released its final report as part of its inquiry into the markets for the supply of AdTech services and ad agency services (**AdTech Report**).

In November 2022, a report on proposed regulatory reforms to address competition and consumer issues that arise in relation to digital platforms was released (**Reform Report**).

Summary:

In the AdTech Report, the ACCC concluded that one company in particular was dominant across the AdTech supply chain, creating significant problems for competition, advertisers, publishers (and ultimately, consumers).

It considered that enforcement action under the *Competition and Consumer Act* 2010 (Cth) was insufficient to address this issue in a timely manner and instead argued that additional ex-ante regulation would be preferable, including:

Empowering the ACCC to:

- Develop sector-specific rules to address conflicts of interest and competition issues applying only to providers that meet criteria related to their market power or strategic position. If such a provision was implemented, rules would be devised in consultation with industry and would need to be proportionate to the risks faced;
- Introduce sector specific rules to allow the ACCC to address competition issues caused by an AdTech provider's "data advantage". These measures should apply where the data advantage arises from the AdTech provider's market power and/or strategic position and the data advantage increases the AdTech provider's market power;
- Develop and enforce rules to improve transparency across the AdTech supply chain; and
- Requiring the industry to establish standards to require AdTech providers to publish average fees and "take rates" for AdTech services, and to enable verification of DSP services.

The ACCC also stressed the need for regulatory alignment with other jurisdictions in relation to digital platforms more broadly. To this end, the AdTech Report highlighted the work being undertaken by the UK Competition & Markets Authority, the European Union, Japan and the United States.

Australia

In the Reform Report, the ACCC recommended introducing reforms to combat scams, harmful apps, fake reviews, inadequate dispute resolution processes, and anti-competitive conduct and introduce stronger consumer safeguards, including expanding the scope of the unfair terms regime and introducing service-specific codes.

How could it be relevant for you?

Companies providing or using AdTech or social media services or some other form of digital platform or software-as-a-service should be aware of looming reforms, which may include those proposed by the ACCC and set out in the Report referred to in chapter 4.

Next steps:

The ACCC is due to provide a further report in March 2023 which will further consider regulatory changes needed in respect of social media services as part of its Digital Platform Services Inquiry and will likely propose further reforms. Further changes are also proposed to digital advertising in the Report relating to the Privacy Act (referred to in chapter 4).

In Australia, content moderation issues typically arise out of defamatory, illegal, age-inappropriate, misleading or harmful (for example cyberbullying) content. Updates on the regulation of each are set out below.

Misinformation/Disinformation

Latest developments:

In its Digital Platforms Report, the ACCC recommended that a mandatory code of conduct for the digital platform industry be implemented to govern the handling of complaints about disinformation. In February 2021 (updated October 2021), the non-profit, Digital Industry Group Inc. (**DIGI**), released a voluntary Australian Code of Practice on Disinformation and Misinformation (the **DM Code**), which outlines how the major digital platforms who have signed up to the DM Code will address concerns regarding disinformation and credibility signalling for news content. Until 18 July 2022 DIGI accepted public submissions to inform potential changes to the code which are currently under review within the first review of the DM Code.

In March 2022, the federal government under previous Prime Minister Scott Morrison (**Morrison Government**) announced it would introduce new legislation to combat harmful misinformation and disinformation online. The legislation would give the Australian Communications and Media Authority (**ACMA**) further powers to hold big tech companies accountable for harmful content on their platforms. The Morrison Government also released a report prepared by the ACMA in June 2021 regarding existing disinformation and misinformation regulation. The new federal government led by Prime Minister Anthony Albanese (**Albanese Government**) confirmed on 20 January 2023 that they will also legislate to provide ACMA with new powers to hold digital platforms to account and improve efforts to combat harmful misinformation and disinformation in Australia. The Albanese Government intends to undertake public consultation on the powers through the release of an exposure draft bill in the first half of 2023 and introduce legislation in Parliament later this year following consultation. It is unclear whether these proposals will look similar to the ones proposed by the Morrison Government.

Australia

Regulation of internet intermediaries & online platforms generally

Digital Advertising

Content Moderation - 2/8

Misinformation/Disinformation

Harmful Content: Online Safety Act 2021 (Cth)

Defamation: Social Media (Anti-Trolling) Bill 2022

Summary:

The core objective of the DM Code is to provide appropriate safeguards to prevent harms that may be caused by disinformation and misinformation. Signatories have agreed to:

- Develop and implement measures which aim to reduce the propagation of, and potential exposure of users of digital platforms to, disinformation and misinformation; and
- Provide an annual report to DIGI regarding their progress towards achieving the outcomes contained in the DM Code (which DIGI will publish publicly).

Signatories may (the DM Code provides that digital platforms can opt-out) also agree to:

- Implement and publish policies, procedures and any appropriate guidelines or information:
  - Relating to the prohibition and/or management of user behaviours and/or content that may propagate disinformation and/or misinformation via their services or products;
  - That will enable users to report the types of behaviours and content that violates such policies; and
  - That aim to disrupt advertising and/or monetisation incentives for disinformation;
- Take measures that prohibit or manage the types of user behaviours that are designed to undermine the integrity and security of their services and products;
- Implement measures to enable users to make informed choices about digital content and to access alternative sources of information;
- Develop and implement policies that provide users with greater transparency about the source of political advertising carried on digital platforms; and
- Support and encourage good faith independent efforts to research disinformation and misinformation both online and offline.

The DM Code provides that signatories are not required to (although they may elect to) signal the veracity of content uploaded and shared by their users nor take measures that require them to delete or prevent access to otherwise lawful content solely on the basis that it is or may be misleading or deceptive or false.

In its report, the ACMA expressed concerns about the DM Code, including that:

- Its effectiveness is limited by an excessively narrow definition or interpretation of 'harm'. It said the current requirement that signatories to the DM Code must only act against content if it is reasonably likely to result in 'serious' or 'imminent' harm could result in a narrow interpretation that would likely exclude a range of chronic harms resulting from the cumulative effect of misinformation over time, e.g. reductions in community cohesion and a lessening of trust in public institutions. The ACMA recommends that "imminent" should therefore be removed from the DM Code's definition of harm.

Australia

Regulation of internet intermediaries & online platforms generally

Digital Advertising

Content Moderation - 3/8

Misinformation/Disinformation

Harmful Content: Online Safety Act 2021 (Cth)

Defamation: Social Media (Anti-Trolling) Bill 2022

- It could be strengthened through an opt-out rather than an opt-in model, as signatories should only be allowed to opt out of outcomes where that outcome is not relevant to their services and should also be required to provide justification for that decision.
- Private messaging services should be included within the scope of the DM Code, with appropriate caveats to protect user privacy, given that private messaging apps are increasingly being used to spread misinformation due to their less restrictive content moderation policies.
- The DM Code does not oblige individual signatories to have robust internal complaints processes.

The proposed legislation is likely to comprise the following:

- Empowering the ACMA with new information-gathering powers (including powers to make record keeping rules) to incentivise greater platform transparency and improve access to Australian-specific data on the effectiveness of measures to address disinformation and misinformation;
- Empowering the ACMA with reserve powers to register and enforce industry codes or make industry standards; and
- The establishment of a Misinformation and Disinformation Act Group, which includes participates from the public and private sector and is designed to collaborate and share information on emerging issues and best practice responses to disinformation and misinformation.

How could it be relevant for you?

Digital platforms should be aware that they could be subject to further regulation on online disinformation and misinformation.

Next steps:

The Albanese Government intends to undertake public consultation on the powers through the release of an exposure draft Bill in the first half of 2023 and introduce legislation in Parliament later this year following consultation.

In the meantime, digital platform providers should also be aware of the DM Code and consider whether to sign up to it.

Harmful Content: Online Safety Act 2021 (Cth)

Latest developments:

In June 2021, the federal government passed the *Online Safety Act 2021* (Cth) (**OS Act**) which makes online service providers accountable for the safety of people who use their services. In particular, it regulates cyber-bullying material targeted at children, cyber-abuse material targeted at adults, abhorrent violent conduct, non-consensual sharing of intimate images and sets out basic online safety expectations for social media services, relevant electronic services and designated internet services.

Summary:

The key features of the new OS Act are as follows:

- Hosting service providers, individuals who post the offending material and providers of social media services, relevant electronic services or designated internet services, may be given a removal notice requiring the removal or cessation within 24 hours of hosting:
  - Cyber-abuse material targeted at Australian adults;
  - Cyber bullying material targeted at Australian children; or
  - Intimate images posted without the consent of the person depicted in the image
- Internet service providers may be requested or required to block access to material that promotes, incites, instructs or depicts abhorrent violent conduct;
- Individuals who share or threaten to share intimate images without the consent of the person depicted may be liable to a civil penalty;
- Industry bodies or associations are directed to develop codes to regulate certain types of harmful online material, which are to be registered by the eSafety commissioner;
- Hosting service providers, providers of social media services, relevant electronic service or designated internet services may be given a 'removal notice', providers of internet search engine services may be given a 'link deletion notice' and providers of app distribution services may be given an 'app removal notice' requiring such providers to remove certain material, based on its actual, likely or lack of classification by the Australian Classification Board, within 24 hours; and
- The relevant Minister may determine basic online safety expectations for social media services, relevant electronic services and designated internet services, for example that such providers will take reasonable steps to ensure that end users are able to use the service in a safe manner.

How could it be relevant for you?

A business operating wholly or partly in one of the sectors set out above should be aware of their obligations to comply with the online safety expectations as well as any notices they receive within the short timeframe specified.

Next steps:

The OS Act commenced on 23 January 2022 and separate codes have been developed for different online business sectors (set out below) which outline steps that must be taken to reduce access and exposure to certain types of harmful online material, including child sexual exploitation material and terrorist material.

The different sectors identified by the OS Act are:

- Social media services;
- Relevant electronic services;
- Designated internet services;
- Internet search engine services;
- App distribution services;
- Hosting services;
- Internet carriage services; and
- Manufacturers, suppliers, maintenance and installation providers of equipment as well as operating service providers.

The draft industry codes were published on 1 September 2022 and were subject to public and industry consultation until the beginning of October 2022. The submissions are currently considered by the industry associations responsible for the codes.

The second phase of codes development, focusing on ‘class 2’ content will take place after the first phase is completed.

Defamation: Social Media (Anti-Trolling) Bill 2022

Latest developments:

Following the release of the exposure draft and the public consultation period in late 2021, the Australian Government tabled the Social Media (Anti-Trolling) Bill 2022 (**AT Bill**) in Parliament in February 2022.

The AT Bill deems social media service providers to be publishers of defamatory statements made on their social media sites by third parties in Australia (as opposed to individual owners of social media pages), with a limited defence only available to providers that implement and follow a rigorous defamation complaints handling scheme prescribed by the AT Bill.

Summary:

The AT Bill was introduced after the High Court of Australia's landmark decision in *Fairfax Media Publications v Voller* (2021) 392 ALR 540 (**Voller**), in which the High Court determined that the owners of public Facebook pages were the publishers of defamatory comments made by third parties on those pages. This applied from the moment the comments were posted and regardless of whether the page owners were aware of the comments.

The AT Bill was introduced partly in response to the Voller decision. A key feature of the AT Bill is that it shifts liability as a 'publisher' of defamatory third-party material posted in Australia away from social media page owners and to social media service providers. In the case of "material" "posted in Australia" on a "page" of a "social media service", the "provider" of the social media service is taken to be a publisher of the material. A "social media service" is defined in the AT Bill by reference to the *Online Safety Act* 2021 (Cth), and must have, inter alia, the sole or primary purpose of enabling online social interaction between end-users.

Further, the AT Bill removes the availability of an innocent dissemination defence for providers in any defamation proceedings relating to defamatory material posted in Australia on social media pages. Instead, the AT Bill introduces a conditional defence available to providers only where they implement and comply with a complaints scheme prescribed by the Bill, comply with the Australian nominated entity requirements (discussed further below), and provide information to complainants either through the complaints scheme, or to the court via an "end-user information disclosure order" to assist in identifying and commencing defamation proceedings against a poster.

The AT Bill allows the complainant to regard the providers as 'publishers' for the purpose of defamation proceedings if the original poster cannot be identified. As the explanatory memorandum to the AT Bill mentions, this is to ensure the complainant still has a defendant available if proceedings cannot be commenced against the poster.

How it could be relevant for you?

The AT Bill confirms that providers of social media services that facilitate social interaction between end-users are liable as publishers for defamatory statements made online. Sites which rely upon anonymous contributions will be affected, as the AT Bill incentivises the collection of personal information. However, within this framework, the AT Bill provides an opportunity for digital platforms to minimise exposure to and liability for defamation proceedings, provided they establish a complaints scheme compliant with the AT Bill and can provide contact details. In tandem with the complaints scheme, in order for a provider to access the conditional defence, the AT Bill requires social media companies of a certain size (250,000 Australian account holders) to establish an Australian-based nominated entity that can fulfil important requirements, such as location data and access to users' relevant contact information.

Next steps:

The AT Bill did not pass into law before the federal election. It is unlikely that the AT Bill will be re-introduced into Parliament by the new Albanese Government, given the party's previous opposition to it.

The AT Bill was examined by the House Select Committee on Social Media and Online Safety, and the Legal and Constitutional Affairs Legislation Committee. Both Committees released their final reports in March 2022.

Separately, the Stage 2 Review of the Model Defamation Provisions reform process commenced in April 2021. These reforms focus on internet intermediary liability for the publication of third-party content as well as the impact of defamation law on reports of alleged criminal conduct and professional misconduct.

In August 2022, the the Standing Council of Attorneys-General released drafts of Model Defamation Amendment Provisions (Part A and Part B) together with accompanying background papers. A range of reforms are proposed to address the problem of intermediary liability for third-party content including a conditional, statutory exemption for a narrow group of internet intermediary function, two alternative options for a new defence for internet intermediaries, clarification and enhancement of court powers and mandatory requirements for an offer to make amends to be updated for online publications.

Part A of the Review of the Model Defamation Provisions centred on internet intermediary liability in defamation for the publication of third-party content. The amendments include statutory exemptions from defamation liability for a narrow group of internet intermediaries, including search engines (in certain circumstances); and a new court power to make orders against non-party internet intermediaries to prevent access to defamatory matter online, amongst other amendments.

On 9 December 2022, the Standing Council of Attorney-Generals approved in principle these amendments, which is subject to final approval in the first half of 2023.

China

Data and evolving digital regulation: algorithm regulation - 1/4

Latest developments:

On 1 November 2021, the *Personal Information Protection Law* (**PIPL**) came into effect. The PIPL has a specific provision for "automated decision-making".

On 31 December 2021, the Cyberspace Administration of China (**CAC**) released the *Administrative Provisions on Algorithm Recommendation of Internet Information Services* (Algorithm Provisions). The Algorithm Provisions came into force on 1 March 2022 and apply to the provision of Internet information services by applying recommendation algorithm technology (Recommendation Algorithm-Based Services) within the territory of China. Recommendation algorithm technology refers to generation and synthesis technology, personalised pushing technology, ranking and selection technology, retrieval and filtering technology, and dispatching and decision-making technology. The Algorithm Provisions mainly set out technical and policy requirements, assessment and content moderation obligations, ecosystem management, user right enhancement and transparency principles, ethical requirements, and filing regime applicable to large platforms. Non-compliance with the Algorithm Provisions may lead to warning, order for rectification, suspension of business in serious cases, and a fine of up to CNY 100,000.

On August 12, 2022, the CAC issued the *Filing List of Domestic Internet Information Service Algorithms (August 2022)* (Algorithm Filing List), publicising the names, uses, application products, record numbers and other information of 30 algorithms from 24 companies that have registered for algorithms. This important law enforcement action also plays an important role in the understanding and application of the Algorithm Provisions.

Summary:

When developing algorithm products or services in China, enterprises should pay attention to the following:

Management measures

- **Institutional and technical measures:** According to Article 7 of the Algorithm Provisions, an algorithm-recommended service provider shall establish and improve management systems and technical measures for examination of algorithm mechanisms and mechanics, scientific and technological ethics review, user registration, examination of information releases, data security and personal information protection, combat against telecommunication network frauds, security assessment and monitoring, emergency response to security incidents, and the like, formulate and publicly disclose rules related to algorithm-recommended services, and assign professionals and technical support commensurate with the scale of algorithm-recommended services.

China

Data and evolving digital regulation: algorithm regulation - 2/4

- **Algorithm evaluation:** According to Article 8 of the Algorithm Provisions, an algorithm-recommended service provider shall regularly review, assess, and verify algorithm mechanisms and mechanics, models, data, and application results, among others.

- **User model and tag management:** According to Article 10 of the Algorithm Provisions, an algorithm-recommended service provider shall improve the rules of points of interest recorded in user models and rules for the management of user tags, and shall not include illegal and negative information as keywords in a user's points of interest or take it as user tags, on the basis of which information is pushed.

- **Prevention of algorithm abuse:** According to Article 6, 8, 14 and 15 of the Algorithm Provisions, an algorithm-recommended service provider shall not use algorithm-recommended services to engage in activities prohibited by laws and administrative regulations; shall not set up algorithm models which induce users to indulge or engage in overconsumption, or otherwise violate laws, regulations, or ethics; shall not use algorithms to falsely register accounts, illegally trade accounts, manipulate user accounts, or falsely send likes, comments, or reposts, or to block information, excessively make recommendations, manipulate lists or the ranking of search results, control trends or selections, or otherwise intervene in the presentation of information and perform acts that influence online public opinion or evade supervision and administration; shall not use algorithms to unreasonably restrict other Internet information service providers, or to obstruct or destroy the normal operation of Internet information services legally provided by them, and to exercise monopoly and unfair competition.

Content review

- **Establish and improve algorithm review to identify illegal and bad information:** According to Article 9 of the Algorithm Provisions, an algorithm-recommended service provider shall establish and improve feature library for identifying illegal and negative information, take measures (stop transmission, prevent proliferation, etc.) when identifying illegal and bad information, keep records and report to competent authorities,

User rights protection

- **Improve the transparency of algorithms, formulate and publish rules related to algorithm recommendation services:** According to Article 16 of the Algorithm Provisions, an algorithm-recommended service provider shall notify users in a conspicuous manner of its provision of algorithm-recommended services, and publish the basic principles, purposes, and main mechanics of algorithm.

- **Ensuring fair trade:** According to Article 7 of the Algorithm Provisions, an algorithm-recommended service provider shall not use algorithms to commit unreasonable differential treatment based on their preferences, transaction practices, and other characteristics.

- **Protection of users' personal information: According to Article 55 of the PIPL, those who use personal information to make automated decisions should:** (a) conduct a Personal Information Protection Impact Assessment (PIPIA), take effective protection measures based on the assessment results, and record the processing activities; (b) conduct PIPIAs on a regular basis (at least once a year) during use of

China

Data and evolving digital regulation: algorithm regulation - 3/4

an algorithm, and improve protection measures based on the assessment results; (c) provide a complaint channel for the results of automatic decision-making, and support manual review of results. Individuals have the right to request an explanation of decisions made by automated decision-making methods that have a significant impact on personal rights, and have the right to refuse decisions made only by automated decision-making.

- **Guaranteeing complaint channels:** According to Article 22 of the Algorithm Provisions, an algorithm-recommended service provider shall set up convenient and effective portals for user complaints and public complaints and reports, specify handling processes and time limit for feedback, and give feedback on the results of handling such complaints and reports in a timely manner.

Special protection for particular groups

- **Protection of minors:** According to Article 18 of the Algorithm Provisions, an algorithm-recommended service provider shall neither push to minors' information which may cause them to imitate unsafe acts or those contrary to social ethics, induce them to develop bad habits, or otherwise affect their physical and mental health nor use algorithm-recommended services to induce them to indulge online.

- **Protection of the elderly:** According to Article 19 of the Algorithm Provisions, an algorithm-recommended service provider shall monitor, identify, and dispose of information related to telecommunications network frauds in accordance with the law, and facilitate their safe use of algorithm-recommended services.

- **Protection of workers:** According to Article 20 of the Algorithm Provisions, an algorithm-recommended service provider which provides workers with job scheduling services shall protect workers' lawful rights and interests in obtaining remuneration of labour, rest, and vacation, among others, and establish and improve platform order distribution, composition and payment of remuneration, working hours, rewards and punishments, and other related algorithms.

Algorithm filing and security assessments

- According to Article 24 and 27 of the Algorithm Provisions, an algorithm-recommended service provider with public opinion attributes or social mobilisation capabilities shall submit its information on the Internet Information Service Algorithm Filing System within ten working days of the date of providing services, and conduct security assessments in accordance with the relevant provisions.

- According to the filing results shown in the Algorithm Filing List, algorithm services with public opinion attributes or social mobilisation capabilities include not only APPs for e-commerce, life, news, information, videos, search engines, social networking, and office, websites, but also the APP for dispatching orders for takeaway riders, the browser APP and the smart TV APP. According to our understanding, the scope of "algorithm services with public opinion attributes or social mobilisation capabilities" is relatively broad. Thus, any platforms that provide users with interactive and information services through the Internet are likely to be subject to algorithm filing and security assessments.

China

Data and evolving digital regulation: algorithm regulation - 4/4

- In addition, according to the filing results shown in the Algorithm Filing List, the scope of "the recommendation algorithms technology" is also broad. As we mentioned above, the recommendation algorithms technology refers to generation and synthesis technology, personalised pushing technology, ranking and selection technology, retrieval and filtering technology, and dispatching and decision-making technology. In the Algorithm Filing List, speech-to-text algorithms are classified as the generation and synthesis technology, and algorithms that only predict the delivery time of orders without actually making decisions are classified as dispatching and decision-making technology. Therefore, it is likely that more types of algorithm-based services will be subject to the Algorithm Provisions in the future.

How could it be relevant for you?

Companies that provide algorithm recommendation services within China should comply with the legal obligations under the Algorithm Provisions, including but not limited to establishing and improving algorithm management systems and technical measures, disclosing the relevant rules for algorithm-recommendation services, optimising algorithm models to present the information that corresponds to mainstream value orientation, and safeguarding users' rights to be informed, to opt-out, to delete personal characteristics and to not be subject to "differentiated treatment." Additionally, providers of algorithm recommendation services with an attribute of public opinion or social mobilisation capability shall complete algorithm self-assessment and file their algorithms with the authority.

Next steps:

At present, the Chinese government's overall approach to algorithm regulation is to give priority to content management to supervise algorithms, taking into account other fields and scenarios, and emphasising the protection of the rights and interests of special groups.

At the same time, according to the current law enforcement trends and policy documents, the focus of work in the next few years will be on: (1) monitoring algorithm security risks; (2) conducting algorithm security assessments; (3) advancing algorithm filing.

Singapore

Content Regulation

New Online Safety Law - 1/2

Foreign Interference (Countermeasures) Act

Singapore has taken various recent legislative and regulatory initiatives to address content issues relevant to digital platforms. Two recent initiatives are set out below.

Latest developments:

On 9 November 2022, the Singapore Parliament passed the Online Safety (Miscellaneous Amendments) Bill to tackle online harms and strengthen online safety for users. The new law took effect on 1 February 2023.

The Bill amends the Broadcasting Act 1994 by introducing a new Part 10A regulating online communication services. It follows on from a public consultation launched in July 2022 on Enhancing Online Safety for Users in Singapore.

Summary:

Online communications services (as specified from time to time) will be required to remove egregious content if directed by the Infocomm Media Development Authority (**IMDA**). Currently, the new law applies to social media services which is the only specified online communication service.

"Egregious content" includes content that advocates or provide instructions on suicide or self-harm, physical or sexual violence, and terrorism, as well as matters that cause racial and religious disharmony in Singapore. If such content is used in a positive way or is educational in nature, such as being mentioned on online forums for users to share personal experiences to help others in overcoming it, it will not be considered harmful or egregious.

Online communication services will be required to block access by Singapore users to such egregious content where directed to do so by the IMDA. A failure to comply with a blocking direction from the IMDA is an offence and may result in a fine of up to SGD 1 million (approximately USD 700,000 or EUR 700,000).

The IMDA may also designate certain online communications services as Regulated Online Communication Services (**ROCS**). These are expected to include services with "significant reach" such as the most widely used social media platforms. ROCS will be required to comply with additional Online Codes of Practice issued by the IMDA.

The IMDA has issued a draft Code of Practice for Online Safety (CPOS), which is expected to come into force in the 2nd half of 2023, following industry consultations by the IMDA. The CPOS will set out obligations for designated social media services to enhance online safety and prevent harmful content on their platforms.

Singapore

Content Regulation

New Online Safety Law - 2/2

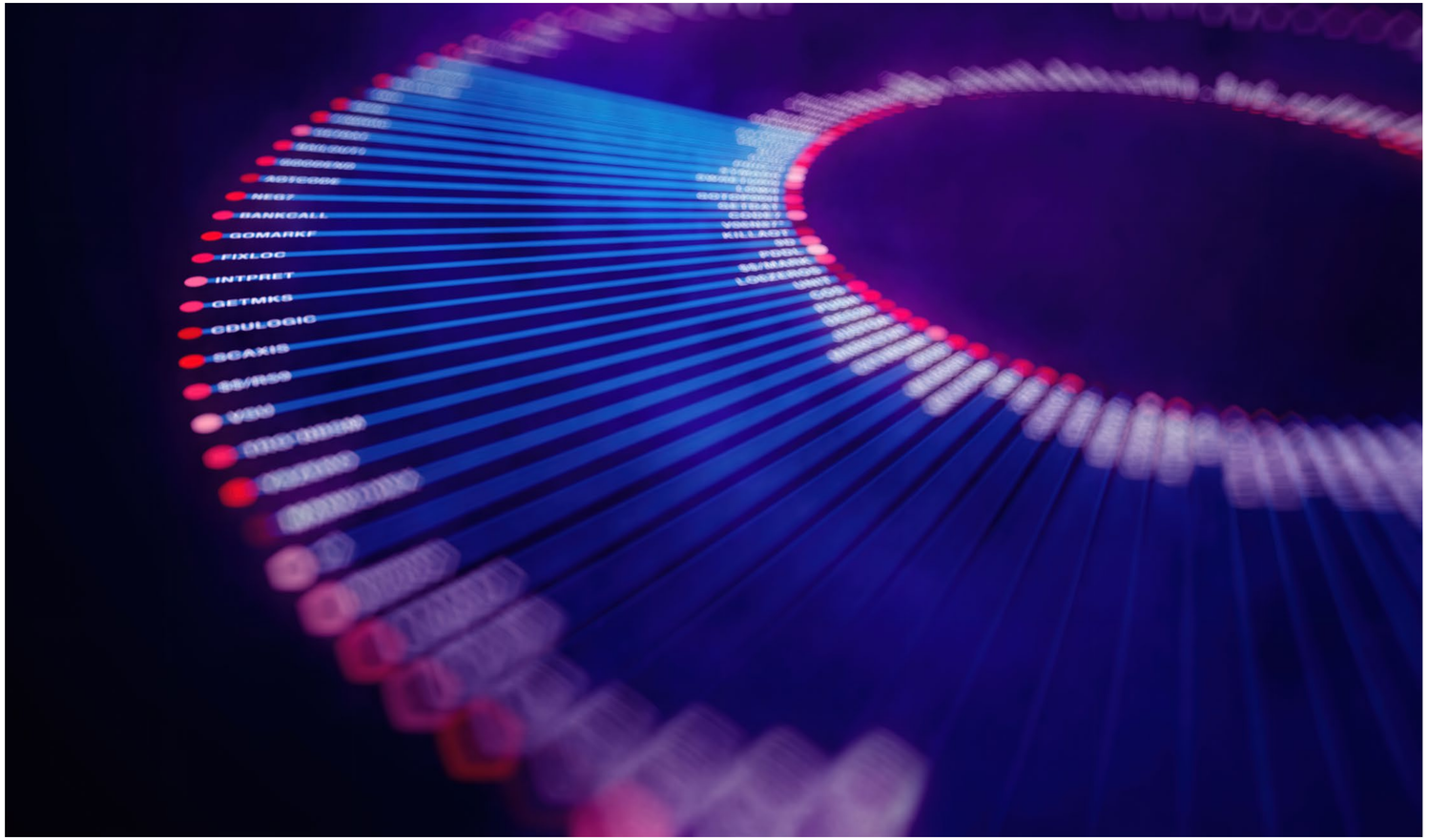
Foreign Interference (Countermeasures) Act

How could it be relevant for you?

Social media platforms will be required to remove egregious content if directed by the IMDA. Social media platforms with significant reach may also be required to take additional measures to comply with requirements under the new Codes of Practice once they are issued.

Next steps:

The IMDA is expected to undertake further consultations on the proposed CPOS. According to the IMDA, the CPOS is expected to be brought into force in the second half of 2023.



Singapore

Content Regulation

New Online Safety Law

Foreign Interference (Countermeasures) Act - 1/2

Latest developments:

Legislative provisions intended to tackle the risk of hostile information campaigns being conducted on online media under the Foreign Interference (Countermeasures) Act 2021 (**FICA**) have come into effect on 7 July 2022.

Summary:

FICA is intended to address (amongst other things) hostile information campaigns involving the use of online tools and tactics to carry out online communications activity by or on behalf of foreign principals contrary to the public interest. Examples of such activity include:

- Creating and using inauthentic accounts to mislead users about the identity and credibility of hostile foreign actors;
- Using bots on social media platforms or taking out advertisements to artificially boost the reach of these messages;
- Using inauthentic accounts and bots in combination to engineer an artificial sense that there is strong public support or opposition to a certain position or sentiment;
- Inciting other users to “troll”, harass or intimidate a particular target; and
- Creating accounts or pages and cultivating a public following by posting on benign topics such as fashion and lifestyle, before using the same accounts or pages to push out political messages subsequently.

Under FICA, the Minister for Home Affairs may authorise a competent authority to issue directions to various entities such as social media services, relevant electronic services, Internet access services, and persons who own or run websites, blogs or social media pages, to assist the authorities to investigate and counter online hostile information campaigns. These may include directions to remove or block content, provide information on harmful communications activity, and disable user accounts.

Singapore

Content Regulation

New Online Safety Law

Foreign Interference (Countermeasures) Act - 2/2

How could it be relevant for you?

Electronic platforms and service providers may be required to comply with requirements to assist authorities to investigate and counter online hostile information campaigns, in addition to other existing laws and regulations governing online content.

Next steps:

The provisions dealing with online hostile information campaigns are the first under FICA to be brought into effect. Separate FICA provisions dealing with other subject matter will be brought into effect subsequently.

Crypto assets

CHAPTER 2

Australia

Hong Kong

Singapore

Australia

Crypto assets - 1/3

Latest developments:

The market for cryptocurrencies and other digital assets is developing rapidly with the government reporting that 25% of Australians held or have previously held cryptocurrencies. In December 2021, the Morrison Government agreed in-principle to recommendations made by the Select Committee on Australia as a Technology and Financial Centre on 20 October 2021 (**Crypto Report**) in relation to consulting on a licensing and custody regime for crypto asset secondary service providers (**CASSPrs**). On 21 March 2022, the Treasury released a consultation paper on the government's proposed approach to licensing crypto asset secondary service providers (**Consultation Paper**).

On 21 March 2022, the Morrison Government requested that the Council of Financial Regulators (**CFR**) give advice on de-banking for digital currency exchanges, FinTech firms, and remittance providers. The Morrison Government also commissioned a report, and issued terms of reference for a review, from the Board of Taxation on the taxation of digital transactions and assets (e.g. crypto).

In August 2022 the Board of Taxation published its Consultation Guide for the review of the tax treatment of digital assets and transactions (Consultation Guide). The submissions were due by the conclusion of September. In late 2022 the CFR published their advice including four key proposals:

- Collect de-banking data;
- Introduce transparency and fairness measures;
- Advise the major banks of the Government's expectation that they provide guidance on their risk tolerance and requirements to the affected sectors; and
- Consider funding capability uplift within the affected sectors.

During the same period, the Treasury commenced a public consultation paper on 'token mapping' to identify areas of reform, licensing frameworks, review innovative organisational structures, and to examine custody obligations for third party custodians.

The ACCC has also recently commenced proceedings against Meta Platforms, Inc and Meta Platforms Ireland Limited in relation to scam celebrity cryptocurrency advertisements (see **chapter 7** for further detail).

Australia

Crypto assets – 2/3

Summary:

The Crypto Report defines cryptocurrency as any form of digital currency that is not reliant on a bank or central authority, but rather uses cryptography.

The Crypto Report recognises the potential of blockchain technology and decentralised finance. However, it found that Australia hasn't yet introduced fit-for-purpose regulatory systems, in contrast with other jurisdictions. The Crypto Report generally covers a range of topics including cryptocurrencies and digital assets, the 'de-banking' of Australian FinTechs, policy relating to neobanks, and the Offshore Banking Unit.

The Committee makes a number of recommendations, including to:

- Introduce a license regime for Digital Currency Exchanges (**DCEs**), noting that DCEs are required to obtain regulatory licenses in some other countries;
- Undertake a 'token mapping exercise' to categorise different crypto-asset tokens;
- Introduce a regime for custodial and depository services for digital assets;
- Introduce a 'Decentralised Autonomous Organisation' legal structure which could assist blockchain-based organisations to operate in Australia;
- Review the Anti-Money Laundering and Counter-Terrorism Financing regulations; and
- Clarify taxation rules for digital assets (among others).

Some of these recommendations, such as the proposal to introduce a licensing regime for DCEs, could have a significant impact on regulation in the digital assets sector. It could also mark a shift in regulation in the digital assets sector, which is mostly unregulated.

Broadly, the Consultation Paper is considering:

- The regulation of CASSPrs who offer crypto asset custody, storage, brokering, exchange and dealing services, or operate a market in crypto assets for retail consumers, including the potential scope and obligations on providers;
- How to categorise and classify crypto assets to provide more certainty to CASSPrs, consumers and regulators. Feedback on a token mapping exercise will be considered as a part of a separate, future consultation process that will be finalised by the end of 2022; and
- The implementation of mandatory minimum, principles-based custody obligations for private-keys that are held or stored by CASSPrs on behalf of consumers.

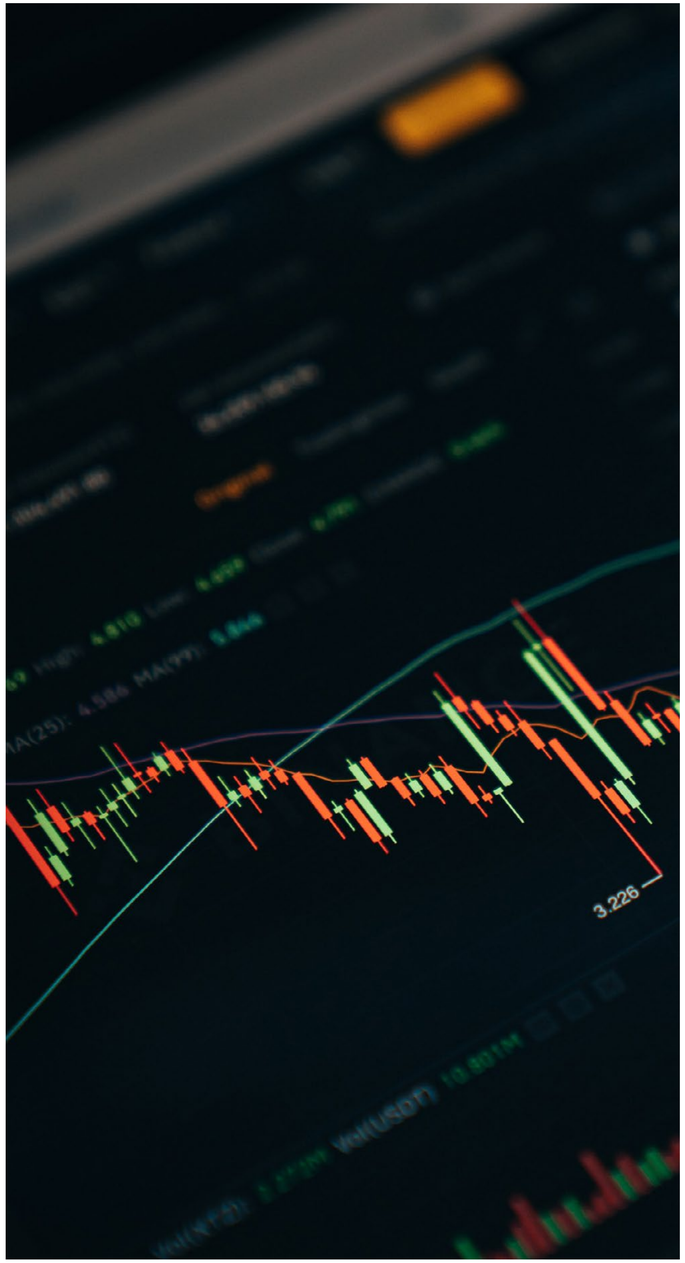
Australia

Crypto assets - 3/3

Next steps and relevance:

Submissions on the proposals and options discussed in the Consultation Paper closed on 27 May 2022. The Treasury is expected to provide advice to the government by mid-2022. Businesses operating in this space should be alert to further regulatory developments. At this stage, it is unclear how the Albanese Government will approach crypto-asset regulation, but it has signalled that it will begin consultation with stakeholders on a regulatory framework for the crypto sector. The new Albanese Government has recognised that the crypto sector is largely unregulated and will engage in a 'token mapping' exercise to help identify how crypto assets and related services should be regulated. This will culminate in the release of a consultation paper in early 2023 to inform what digital assets should be regulated by financial services laws and will form the foundation for a future custody and licensing framework in 2023 before introducing legislation.

In the area of competition and consumer law, the ACCC's enforcement and compliance priorities for 2022-2023 include a focus on the financial services sector. The ACCC is set to prioritise 'promoting competition and investigating allegations of anti-competitive conduct' in the sector, particularly in relation to payment services.



Hong Kong

Licensing regime for Virtual Asset Service Providers - 1/3

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins

Latest developments:

Since 6 November 2019, the Securities and Futures Commission (**SFC**) has adopted an opt-in regime under which virtual asset trading platform (**VATP**) operators may voluntarily elect to be regulated by the SFC if they permit the trading of at least one securities token on their platform. However, due to its voluntary nature, VATP operators can avoid SFC oversight by limiting the nature of the tokens traded on their platform.

On 7 December 2022, the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 (**AMLO Amendment Bill**) which sets out the Virtual asset service providers (VASP). licence regime was passed by the Legislative Council, and will take effect on 1 June 2023 (**Commencement Date**).

As part of the licensing regime, the SFC will be empowered to impose conduct requirements on, and exercise supervisory and disciplinary powers in respect of, licensed VASPs. On 20 February 2023, SFC published the Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission in preparation for commencement of the law (**Consultation Paper**).

Summary:

(i) The Licensing Regime

The licensing regime under the AMLO Amendment Bill will apply to:

- Any person in Hong Kong that carries on a business of providing any VA service or holds themselves out as carrying on a business of providing any VA service; and
- Any person outside Hong Kong that (i) actively markets to the public in Hong Kong any services the person provides or purports to provide, and (ii) the provision of such services, if done in Hong Kong, would constitute providing a "VA service".

"Virtual assets" (VA) refers to digital representations of value which may be in the form of digital tokens or any other virtual commodities, crypto assets or other assets of essentially the same nature, irrespective of whether or not they amount to "securities" or "futures contracts" as defined under the Securities and Futures Ordinance (SFO) but excludes digital representations of fiat currencies issued by central banks.

Whether non-fungible tokens (NFT) fall within the scope of VA depends on its terms and features. NFTs that are "genuine digital representation of a collectable" would unlikely fall within the definition of VA.

It is important to note that there is power under the AMLO Amendment Bill for the Secretary for Financial

Hong Kong

Licensing regime for Virtual Asset Service Providers - 2/3

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins

Services and the Treasury to prescribe by notice any digital representation of value to be a VA or not, either generally or in any particular case.

"VA service" is defined to mean operating a VA exchange, that is to say, providing services through means of electronic facilities-

- Whereby-
  - Offers to sell or purchase VA are regularly made or accepted in a way that forms or results in a binding transaction; or
  - Persons are regularly introduced, or identified to other persons in order that they may negotiate or conclude, or with the reasonable expectation that they will negotiate or conclude sales or purchases of VA in a way that forms or results in a binding transaction; and
- Where client money or client VA comes into direct or indirect possession of the person providing such service.

Based on the above definition of "VA service", virtual asset payment systems and virtual asset custodian services are unlikely to be in-scope for licensing purposes.

In summary, the features of the licence regime include the following:

- The applicant must be either a Hong Kong incorporated company or an overseas company that is registered as a non-Hong Kong company under the Companies Ordinance.
- The SFC must be satisfied that the applicant is "fit and proper".
- The applicant must have at least 2 persons who will act as "responsible officers" of the applicant.
- The SFC must be satisfied that each director of the applicant is a fit and proper person to be associated with the business of providing the relevant VA services.
- The SFC must be satisfied that the "ultimate owner" (if any) of the applicant is a fit and proper person to be associated with the business of providing the relevant VA services. The "ultimate owner" of the applicant is "an individual who:
  - Owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;
  - Is, directly or indirectly, entitled to exercise or control the exercise or more than 25% of the voting rights at general meetings of the corporation; or
  - Exercises ultimate control over the management of the corporation".
  - A person may not become the ultimate owner of a licensed provider unless that SFC has given its approval to such person.
- The SFC must approve the premises to be used by the applicant for keeping records and documents required under the licensing regime.

Hong Kong

Licensing regime for Virtual Asset Service Providers – 3/3

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins

- Specific requirements will be introduced for customer due diligence.

- Licensed VASPs are only allowed to provide services to *professional investors* (hence must block access to the platform for any investors who do not meet the professional investor criteria).

Since the regulator is the **SFC**, applicants for a licence must comply with SFC codes, guidelines and circulars relating to VA licensees, in addition to complying with the statutory requirements under the AMLO Amendment Bill.

(ii) Regulation of virtual assets market misconduct

The AMLO Amendment Bill includes offences for market misconduct related to VAs:

- Offence involving fraudulent or deceptive devices in transactions in VAs – this offence is subject to a fine of up to HK$10 million and to imprisonment for up to 10 years;

- Offence to fraudulently or recklessly induce others to invest in VAs – this offence is subject to a fine of up to HK$1 million to imprisonment for up to 7 years.

How could it be relevant for you?

If a VASP is operating an exchange in Hong Kong, it must obtain a license from the SFC. If a license is not obtained, it is expected to cease operations by 1 June 2024. If an unlicensed VASP operates a VA exchange outside Hong Kong but actively markets its services to customers in Hong Kong, it will be considered to have breached the AMLO. Licensed VASPs will have to offboard all retail customers, as they are only permitted to provide services to professional investors.

Next steps:

The licensing regime is proposed to come into effect on 1 June 2023 (Commencement Date). To implement the licensing regime under AMLO, SFC in the Consultation Paper proposes to provide a 12-month transitional period for compliance with the requirements under AMLO. VASPs which are not in operation in Hong Kong before the Commencement Date shall not commence business without being licensed.

Meanwhile, a pre-existing VASP in Hong Kong (i.e. in operation in Hong Kong before the Commencement Date) can continue to operate during the 12-month "non-contravention period" till 31 May 2024. Starting from 1 June 2024 onwards, all VASPs cannot operate in Hong Kong unless it is licensed or deemed to be licensed. To qualify as a deemed licensee, the pre-existing VASP shall submit the licence application by 29 February 2024, and it will be deemed licensed even after the end of the non-contravention period, until the earlier of: (i) the SFC's grant or refusal of its licence; or (ii) the withdrawal of the licence application.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities – 1/5

Proposal to regulate crypto-assets and stablecoins

Latest development:

On 28 January 2022, the Hong Kong Securities and Futures Commission **(SFC)** and the Hong Kong Monetary Authority **(HKMA)** issued a joint circular on intermediaries' virtual asset-related activities **(Joint Circular)**, which supersedes the SFC's circular to intermediaries, being SFC licensed corporations or registered institutions that may conduct regulated activities, on the distribution of virtual asset funds dated 1 November 2018.

Summary:

The Joint Circular provides guidance to SFC-licensed or registered intermediaries that are currently engaged or intends to engage in activities relating to virtual assets (VAs, which may include utility tokens, security- or asset-backed tokens, stablecoins and other crypto assets), including various new requirements to be complied with and best practices. The Joint Circular mainly covers the following activities relating to virtual asset-related products **(VA-related products)** and services:

- Distribution of VA-related products;
- Provision of virtual asset dealing services **(VA dealing services)**; and
- Provision of virtual asset advisory services **(VA advisory services)**.

"VA-related products" is defined to mean products which:

- Have a principal investment objective or strategy to invest in virtual assets;
- Derive their value principally from the value and characteristics of virtual assets; or
- Track or replicate the investment results or returns which closely match or correspond to virtual assets.

The key requirements set out in the Joint Circular are summarised as follows:

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities – 2/5

Proposal to regulate crypto-assets and stablecoins

(i) Distribution of VA-related products

The following requirements are applicable to the distribution of VA-related products:

Requirements	Explanation
Requirements on complex product	VA-related products are highly likely considered as complex products and will be subject to requirements relating to distribution (e.g. ensuring suitability, minimum information and warning statements).
"Professional investors" only	Except for a limited suite of products (e.g. VA-related derivative products that are traded on regulated exchanges specified by the SFC, or exchange-traded VA derivative funds that are authorised or approved for offering to retail investors by the respective regulator in a designated jurisdiction), VA-related products as complex products should only be offered to professional investors.
Virtual asset-knowledge test	Except for institutional professional investors and qualified corporate professional investors, intermediaries should (i) Assess whether clients have knowledge of investing in virtual assets or VA-related products prior to effecting a transaction in VA-related products on their behalf; and (ii) Ensure that their clients have sufficient net worth to be able to assume the risks and bear the potential losses of trading VA-related products. Non-exhaustive criteria for assessing whether a client can be regarded as having knowledge of virtual assets has been set out by SFC.
Financial accommodation	When providing any financial accommodation for investing in VA-related products to clients, an intermediary should be cautious and should assure itself the client has the financial capacity to meet the obligations arising from leveraged or margin trading in VA-related products, including in a worst-case scenario. In the absence of such assurance, the intermediary should not accept instructions from the client.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities – 3/5

Proposal to regulate crypto-assets and stablecoins

Requirements	Explanation
Provision of information in a clear and easily comprehensible manner	Intermediaries should ensure that information relating to VA-related products and the underlying virtual asset investments are provided in a clear and easily comprehensible manner to clients.
Provision of warning statements	Intermediaries should provide warning statements (which can be a one-off disclosure) to clients specific to virtual assets. The warning statements should include without limitation and where applicable, the general risks of trading in futures contracts, risks specific to virtual asset futures contracts, the continuing evolution of virtual assets and how this may be affected by global regulatory developments, price volatility, and other applicable risks.

(ii) Provision of VA dealing services

Intermediaries providing VA dealing services are also required to comply with the following requirements:

Requirements	Explanation
Professional investors only	VA dealing services should only be provided to professional investors.
SFC and HKMA requirements	Intermediaries are expected to comply with all the regulatory requirements imposed by the SFC and the HKMA when providing VA dealing services, regardless of whether the virtual assets involved are securities.
Partner with SFC-licensed VA trading platform	In order to provide VA dealing services, intermediaries are required to partner only with SFC-licensed VA trading platforms.
Existing type 1 clients only	VA dealing services can only be provided to the intermediaries' existing clients to which they provide type 1 (dealing in securities) regulated services.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities – 4/5

Proposal to regulate crypto-assets and stablecoins

Requirements	Explanation
Terms and conditions of licensing / registration	The SFC (in consultation with the HKMA, where applicable) will impose as licensing / registration conditions **(Terms and Conditions)** the expected conduct requirements for intermediaries' provision of VA dealing services under an omnibus account arrangement. The Terms and Conditions subject the intermediaries to various obligations, including only permitting clients to deposit/withdraw fiat currencies from their accounts, and no deposit or withdrawal of client virtual assets will be allowed to minimize risks associated with such transfer.
Terms and conditions for virtual asset discretionary account management services	In respect of virtual asset discretionary account management services, if a licensed corporation intends to invest 10% or more of the gross asset value of a portfolio in virtual assets, additional requirements will apply as set out in the *Proforma Terms and Conditions for Licensed Corporations which Manage Portfolios that Invest in Virtual Assets* which was published in 2019 (**Proforma Terms and Conditions**).

(iii) Provision of VA advisory services

Requirements	Explanation
SFC and HKMA requirements	Intermediaries are expected to comply with all the regulatory requirements imposed by the SFC and the HKMA when providing advisory services irrespective of the nature of the VAs (e.g. whether or not the VAs involved are securities).
Existing type 1 and 4 clients only	VA advisory services should only be provided to intermediaries' existing clients to which they provide type 1 or type 4 (advising on securities) regulated services who are professional investors.
VA-related products requirements	Intermediaries providing advisory services in VA-related products should observe the requirements in relation to VA-related products set out in **chapter 4**.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities – 5/5

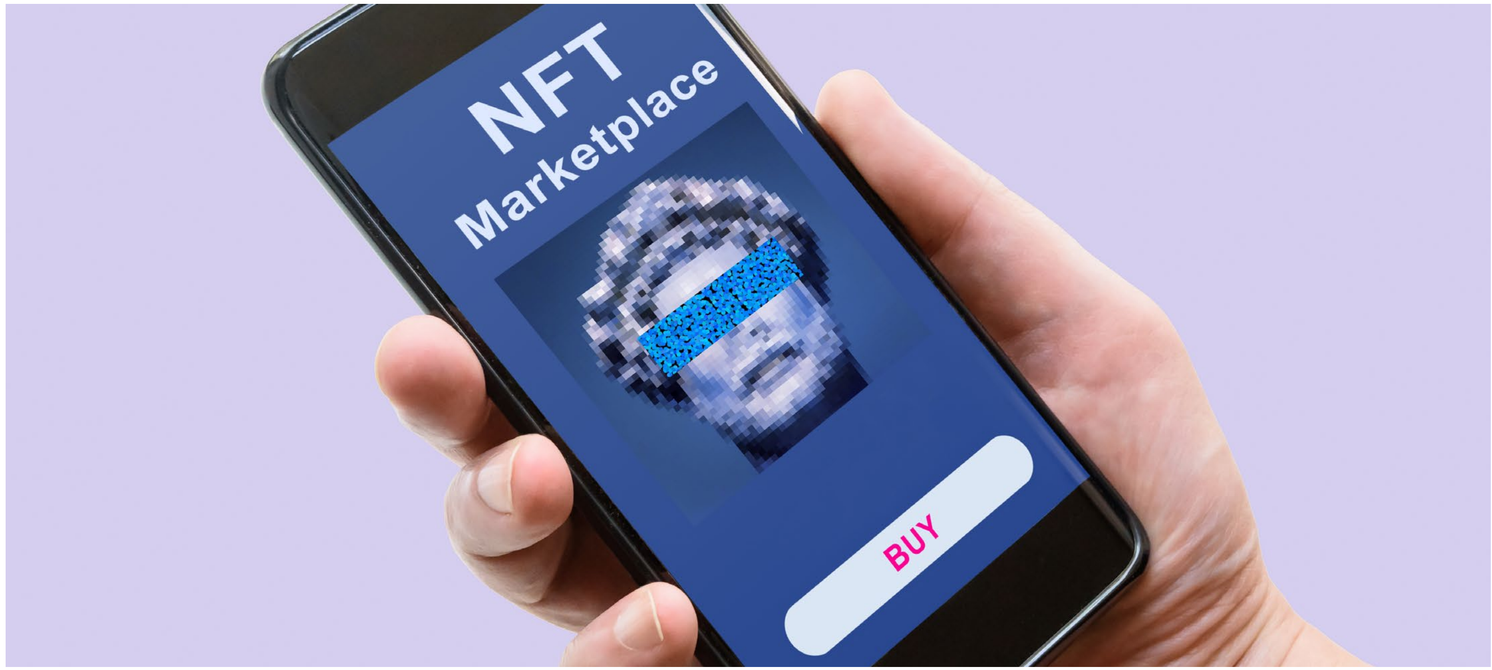
Proposal to regulate crypto-assets and stablecoins

How could it be relevant for you?

Given the implementation timeframe set out above, both intermediaries which currently engage in VA-related activities and those which intend to engage in VA-related activities should immediately assess the relevant VA-related products and services to meet the relevant requirements which will apply pursuant to the Joint Circular. Intermediaries should also ensure that the above-mentioned requirements are properly complied with before the transition period expires.

Next steps:

The Joint Circular will be effective immediately for intermediaries which do not currently engage in VA-related activities. For intermediaries which are serving existing clients of VA-related activities, there will be a six-month transition period for full implementation of the requirements of the Joint Circular, and the Joint-Circular suggests that further guidance may be provided during this transition period. Additional guidance is also expected for practical steps to be taken by the intermediaries already engaging in VA-related activities to update their internal policies and procedures in compliance with the new regulatory requirements.



Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins – 1/4

Latest development:

On 12 January 2022, the Hong Kong Monetary Authority (**HKMA**) issued a "Discussion Paper on Cryptoassets and Stablecoins" (**Discussion Paper**) to invite feedback from stakeholders on a regulation framework for payment related stablecoins that have a potential reach and use across multiple jurisdictions, including as means of making payments and/or stores of value.

After taking into account the feedback received on the Discussion Paper, the HKMA published the consultation conclusion (**Consultation Conclusion**) on 31 January 2023 and sets out its responses.

Summary:

(i) What to regulate

The HKMA will adopt a risk-based approach by giving priority to regulating stablecoins that purport to reference to one or more fiat currencies irrespective of the underlying stabilisation mechanism of that stablecoin. The HKMA perceives this type of stablecoins as potentially posing more imminent monetary and financial risks as they are likely to be used in payments and have linkages with the traditional financial system.

Appropriate flexibility will also be built-in to the proposed regime for HKMA to adjust the scope of regulation down the road in light of rapid market and international developments (e.g. scope in other stablecoin structure(s)).

The HKMA will exclude certain arrangements from the definition of stablecoins. This is intended to avoid regulatory overlap with, for example, the arrangements already being subject to another financial regulatory regime, or used within a well-confined environment outside the reach of the general public. Note that the details of the exclusion will be subject to further analysis and additional consultations to be conducted by the HKMA.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins – 2/4

(ii) Key activities to be regulated

The HKMA proposed to regulate the following key activities (each a **"Regulated Activity"**) in the lifecycle of a stablecoin:

Activities	Explanation
Governance	establishment and maintenance of the rules governing an in-scope stablecoin arrangement
Issuance	issuing, creation or destroying of an in-scope stablecoin
Stabilisation	stabilisation and reserve management arrangements of an in-scope stablecoin (whether or not such arrangements are provided by the issuer)
Wallets	provision of services that allow the storage of the users' cryptographic keys which enable access to the users' holdings of an in-scope stablecoin and the management of such stablecoins

(iii) Which entities to be licensed

The following entities will need to be licensed by the HKMA:

- Entities conducting a regulated activity in Hong Kong in relation to in-scope stablecoins;
- Entities actively marketing such regulated activities to the general public of Hong Kong;
- Entities conducting stablecoin-related activities in which the stablecoin concerned purports to reference its value to the Hong Kong dollar, regardless of whether the relevant regulated activity is conducted in Hong Kong or actively marketed to the general public; or
- Entities in which the authority is of the opinion that should be so regulated, having regard to matters of significant public interest.

The HKMA will introduce flexibility to scope in an entity according to circumstances.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins – 3/4

(iv) Key regulatory principles

The HKMA proposes to regulate each type of Regulated Activity by different licences rather than one single type of licence covering various activities. The regulatory requirements in the licences are still under discussion, but the HKMA considers the following as crucial principles to formulate the regulatory regime:

Principles	Explanation
Comprehensive regulatory framework	The regulatory regime shall cover a broad range of areas such as ownership, governance and management, financial resources requirements, risk management, anti-money laundering and counter-terrorist financing, user protection, and regular audits and disclosure requirements.
Full backing and redemption at par	The value of the reserve assets of a stablecoin arrangement should meet the value of the outstanding stablecoins at all times. The reserve assets should be of high quality and high liquidity. Stablecoins that derive their value based on arbitrage or algorithm will not be accepted. Stablecoin holders should be able to redeem the stablecoins into the referenced fiat currency at par within a reasonable period.
Principal business restriction	The regulated entities should not conduct activities that deviate from its principal business as permitted under their relevant licences. For example, wallet operators should not engage in lending activities.

How could it be relevant for you?

The recent crash of algorithmic stablecoins and the collapse of a major crypto exchange has brought the regulation of stablecoins to the priority. Whilst a greater level of details on the regulatory framework are expected to materialise upon further consultation, the Consultation Conclusions are a helpful indication of the overall regulatory trajectory for crypto-assets and stablecoins in the coming two years.

Hong Kong

Licensing regime for Virtual Asset Service Providers

Updated requirements for Virtual asset related activities

Proposal to regulate crypto-assets and stablecoins – 4/4

Next steps

As highlighted in the Consultation Conclusions, the HKMA currently aims to implement the regulatory regime by 2023/2024. The HKMA will conduct further assessment to avoid regulatory arbitrage, identify and address regulatory overlaps or gaps and mitigate the risks arising from different activities. A more detailed consultation on the draft legislation will be conducted in due course.

The HKMA envisages that the draft legislation will address the following key issues such as

- Defining the structures and activities that would be regulated or not regulated;
- The range of effective and proportionate powers that should be granted to the HKMA;
- The key regulatory requirements;
- The range of powers that should be given to the authority to allow; and
- The relevant guiding factors that the authority should have regard to in exercising the powers under point (d) above

The HKMA notes the way services are provided in the crypto space is evolving rapidly and is monitoring the interconnectedness between other crypto-assets and the mainstream financial system.

Singapore

Licensing of Digital Token Service Providers - 1/2

Guidelines on Provision of Digital Payment Token Services to the Public

Latest developments:

The Financial Services and Markets Act (**FSMA**) was passed by Parliament on 5 April 2022. It provides the Monetary Authority of Singapore (**MAS**) with enhanced powers to regulate the financial sector.

When it comes into effect, the FSMA will (amongst other things) establish a new licensing and regulatory regime for virtual asset service providers (**VASPs**) that provide digital token (**DT**) services to overseas markets from Singapore.

Summary:

One of the aims of the FSMA is to implement enhanced standards on VASP regulation adopted by the Financial Action Task Force (**FATF)** in 2019. In particular, the enhanced FATF standards require VASPs to be at least licensed or registered in the jurisdictions(s) where they are created, in order to address anti-money laundering and counter terrorism financing (**AML/CFT)** concerns and to mitigate the risk of regulatory arbitrage (where no single jurisdiction has sufficient regulatory hold over a specific VASP due to the Internet and digital nature of its business).

Currently, Singapore requires certain VASPs that constitute a digital payment token service under the Payment Services Act 2019 (**PSA)** to be licensed. However, the existing licensing framework under the PSA only requires service providers that carry on business in Singapore to be licensed.

In order to align the Singapore regulatory regime with the enhanced FATF standards, the FSMA will require VASPs that provide DT services outside of Singapore from a place of business in Singapore to be licensed and subject to ongoing regulatory requirements. DT services that will be regulated under the FSMA include:

- Dealing in DTs;
- Facilitating the exchange of DTs;
- Accepting DTs from one DT account for the purposes of transmitting, or arranging for the transmission of, the DTs digital tokens to another DT account;
- Arranging for the transmission of DTs from one DT account to another DT account;
- Inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to buying or selling any DTs in exchange for any money or any other DTs;

Singapore

Licensing of Digital Token Service Providers - 2/2

Guidelines on Provision of Digital Payment Token Services to the Public

- Safeguarding a DT (or DT instrument), where the service provider has control over the DT (or one or more DTs associated with the DT instrument);
- Carrying out for a customer an instruction relating to a DT (or one or more DTs associated with a DT instrument), where the service provider has control over the DT (or the DT instrument); and
- Providing advice in relation to the sale or offer for sale of DTs.

DT service providers licensed under the FSMA will be regulated primarily to address AML/CFT risks. MAS intends for AML/CFT requirements imposed on DT service providers under the FSMA to be aligned with the requirements imposed on digital payment token service providers licensed under the PSA.

How could it be relevant for you?

VASPs that provide DT services to overseas markets from a place of business in Singapore may be subject to new licensing and regulatory requirements when the licensing framework under the FSMA comes into effect.

Next steps:

The provisions establishing a new licensing framework for DT service providers under the FSMA have yet to be brought into force. Details of the new licensing framework are expected to be consulted upon by the MAS, before being set out in subsidiary legislation when the licensing framework is brought into effect.

Singapore

Licensing of Digital Token Service Providers

Guidelines on Provision of Digital Payment Token Services to the Public - 1/2

Latest developments:

On 17 January 2022, MAS issued the Guidelines on Provision of Digital Payment Token Services to the Public (**DPT Guidelines**) to provide clarity and implement MAS' expectation that trading of digital payment tokens (**DPTs**) or cryptocurrencies is not suitable for the general public, and that DPT service providers should not promote their services to the general public.

Summary:

The DPT Guidelines apply to DPT service providers licensed under the PSA, banks and financial institutions providing DPT services in Singapore, as well as DPT service providers operating under a transitional exemption granted by MAS (collectively "**DPT service providers**").

The DPT Guidelines set out MAS' view that the trading of DPTs is seen as a high risk activity and not suitable for the general public, and that the public should not be encouraged to engage in the trading of DPTs.

Under the DPT Guidelines, DPT service providers:

- Should not portray the trading of DPTs in a manner that trivialises the high risks of trading in DPT;
- Should not promote their DPT services in public areas in Singapore or through any other media directed at the general public in Singapore, including placing advertisements or promotional materials in public areas such as Singapore public transport, public transport venues, broadcast media or periodical publications, third party websites, social media platforms, public events or roadshows;
- May promote their services on their own corporate website, mobile applications, or official social media accounts, provided they do not trivialise the risks of trading in DPTs;
- Should not engage third parties, such as social media influencers or third-party websites, to promote their DPT services to the general public in Singapore, including joint promotional campaigns to solicit new customers;
- Should not provide physical ATMs in public areas in Singapore to facilitate public access to their DPT services; and
- Should not promote payment token derivatives (**PTDs)**, i.e., derivatives contracts that reference DPTs as underlying assets, to the public as a convenient alternative to trading in DPTs, and should not mislead the public that PTDs are less risky than DPTs.

Singapore

Licensing of Digital Token Service Providers

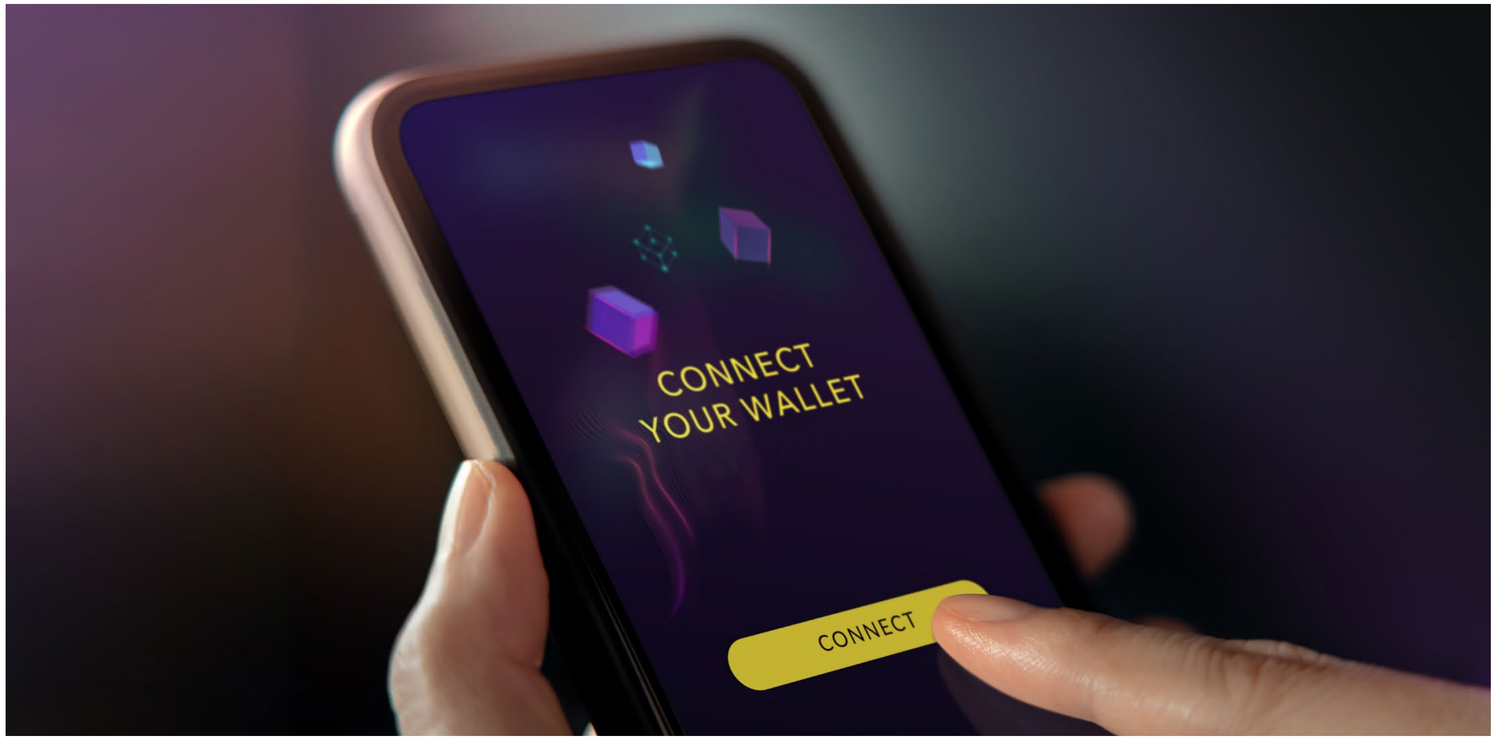
Guidelines on Provision of Digital Payment Token Services to the Public - 2/2

How could it be relevant for you?

DPT service providers should be aware of the existing restrictions against promoting DPT services to the public under the DPT Guidelines, and monitor this area for further regulatory developments in light of MAS' stated policy intent to introduce further measures.

Next steps:

In August 2022, the Managing Director of MAS publicly announced that the position of MAS is to seek to promote innovations in tokenisation and distributed ledger technologies, while strongly discouraging and seeking to restrict speculation in cryptocurrencies. It was further mentioned that MAS is considering further measures to reduce risk of harm to consumers arising from cryptocurrency trading, such as by introducing customer suitability tests and restricting the use of leverage and credit facilities for cryptocurrency trading.



AI as a digital asset

CHAPTER 3

Australia

China

Hong Kong

Singapore

Guidance on Ethical Development and Use of AI

Study on “Fostering Consumer Trust - Ethical AI in Hong Kong”

Australia

Regulation of AI - 1/2

Liability regime for AI

Latest developments:

In March 2022, the Morrison Government released an issues paper seeking views on regulatory settings and systems that can enable and better facilitate the responsible use of artificial intelligence (**AI**) and automated decision-making (**ADM**) in Australia (**Issues Paper**).

The ACCC's Digital Platforms Reports also considered emerging developments in relation to AI and its use by digital platforms.

Summary:

The Issues Paper notes that 'new and emerging technologies are challenging approaches to regulation' and that 'unclear or outdated legislation, or poor understanding of requirements under these laws, may impose a barrier to the adoption of these technologies and can undermine public trust and confidence' in AI and ADM.

Opportunities for reform highlighted in the Issues Paper include:

- Clarifying the application of existing regulation of AI and ADM, which could include the provision of guidance on the application of existing legislation;
- Addressing inconsistent or overlapping regulation;
- Ensuring current and new regulations are technology-neutral;
- Identifying where new regulation may be required to minimise existing and emerging risks; and
- Driving best shared practice and implementation across government and industry.

The AI Action Plan will be implemented under four focus areas:

- The development and adoption of AI to transform businesses;
- The creation of an environment to grow and attract the world's best AI talent;
- The use of cutting-edge AI technologies to solve Australia's national challenges; and
- Making Australia a global leader in responsible and inclusive AI by providing support to ensure AI technologies are built to reflect Australian values.

Australia

Regulation of AI - 2/2

Liability regime for AI

It will be implemented through a combination of AI direct measures programs and incentives that drive the growth of AI, and foundational policy settings that support businesses, innovation and the economy to further the development of AI.

Outside the federal government's voluntary AI Ethics Framework (containing eight principles designed to help organisations developing or implementing of AI to reduce the risk of its negative impacts ensure that its use is supported by good governance standards) Australia does not yet directly regulate AI. However, various other legislation may indirectly regulate AI, for example via the Privacy Act or civil liability statutes.

AI was also featured in the ACCC's Digital Platforms Report. The ACCC supported expanding the definition of 'personal information' in the Privacy Act to align with the definition of 'personal data' in the GDPR to address challenges posed by emerging technologies such as AI and data analytics (such proposition is included in the Report referred to in chapter 4 of this guide).

The Digital Platforms Report also considered emerging developments in online news and AI, noting that although AI, machine learning and chatbots can have positive applications in news production and in counteracting the spread of misinformation and disinformation, these technologies also have the potential to cause harm, particularly in relation to scams and fraudulent economic and social activities. The ACCC observed that the increasing use of AI in news production and consumption may raise issues of 'AI bias', where AI systems containing statistical biases in their models or algorithms could lead to undesirable, unequal and unfair outcomes. The ACCC warned that issues of AI bias may lead to "extremely concerning outcomes" if replicated in the socially important functions of producing, distributing and consuming news. It did not make any specific reform recommendations in respect of this issue, however it may be covered in a later report as part of the Digital Platforms Services inquiry referred to in chapter 1.

How could it be relevant for you?

Impacts of proposed reforms to the Privacy Act are discussed in chapter 4 of this guide.

Next steps:

As set out in chapter 4, the Privacy Act is currently under review and subject to a reform process that will likely affect the regulation of AI.

Australia

Regulation of AI

Liability regime for AI - 1/2

Latest developments:

While AI technology brings immense benefits to society, there are circumstances where AI-driven products or services fail. In these circumstances, it is important to consider issues around liability, particularly considering the rapid expansion in the use of AI since the onset of the COVID-19 pandemic.

Summary:

In Australia, there has been some focus by the government on liability for specific AI inventions, such as driverless vehicles. In 2017, the Standing Committee on Industry, Innovation, Science and Resources completed its Inquiry into the Social Issues Relating to Land-Based Driverless Vehicles in Australia which discussed the uncertainty of legal responsibility and insurance in the case of car accidents where there is some automation. The Committee recognised that the introduction of driverless vehicles may require a change 'in the way vehicles are insured and in the current understanding of legal liability'.

Developments are also occurring in relation to AI in the area of intellectual property protection in Australia. For example, there are questions as to whether AI creations might be protected under copyright, since there are requirements that a work is original and originates from an author (and it is necessary to have a human author*). This contrasts with the position in the UK, where works generated by a computer are protected, even if there is no human creator.

On appeal in *Commissioner of Patents v Thaler* [2022] FCAFC 62, the Full Court of the Federal Court of Australia unanimously found that an AI machine cannot be named as an inventor in a patent application, and that the inventor listed in an application for a patent must be a natural person and the High Court of Australia subsequently refused Dr Stephen Thaler's application for special leave to appeal this decision.

While liability has been explored in the context of automated cars, there is no general framework for AI liability. This means that liability regimes for AI can include the areas of tort, product liability, or contract law. In relation to tortious liability, parties who are liable could be extensive and might include, for example, the manufacturer, operator, creator, or owner of the AI.

In many cases, liability for AI products and services is likely to be simple. However, more sophisticated uses of AI could challenge existing liability regimes, and different forms of liability for AI may need to be considered. Some proposals suggest giving AI legal personhood or personality, or introducing strict liability regimes for AI.

*IceTV Pty Ltd v Nine Network Australia Pty Ltd (2009) 239 CLR 458.

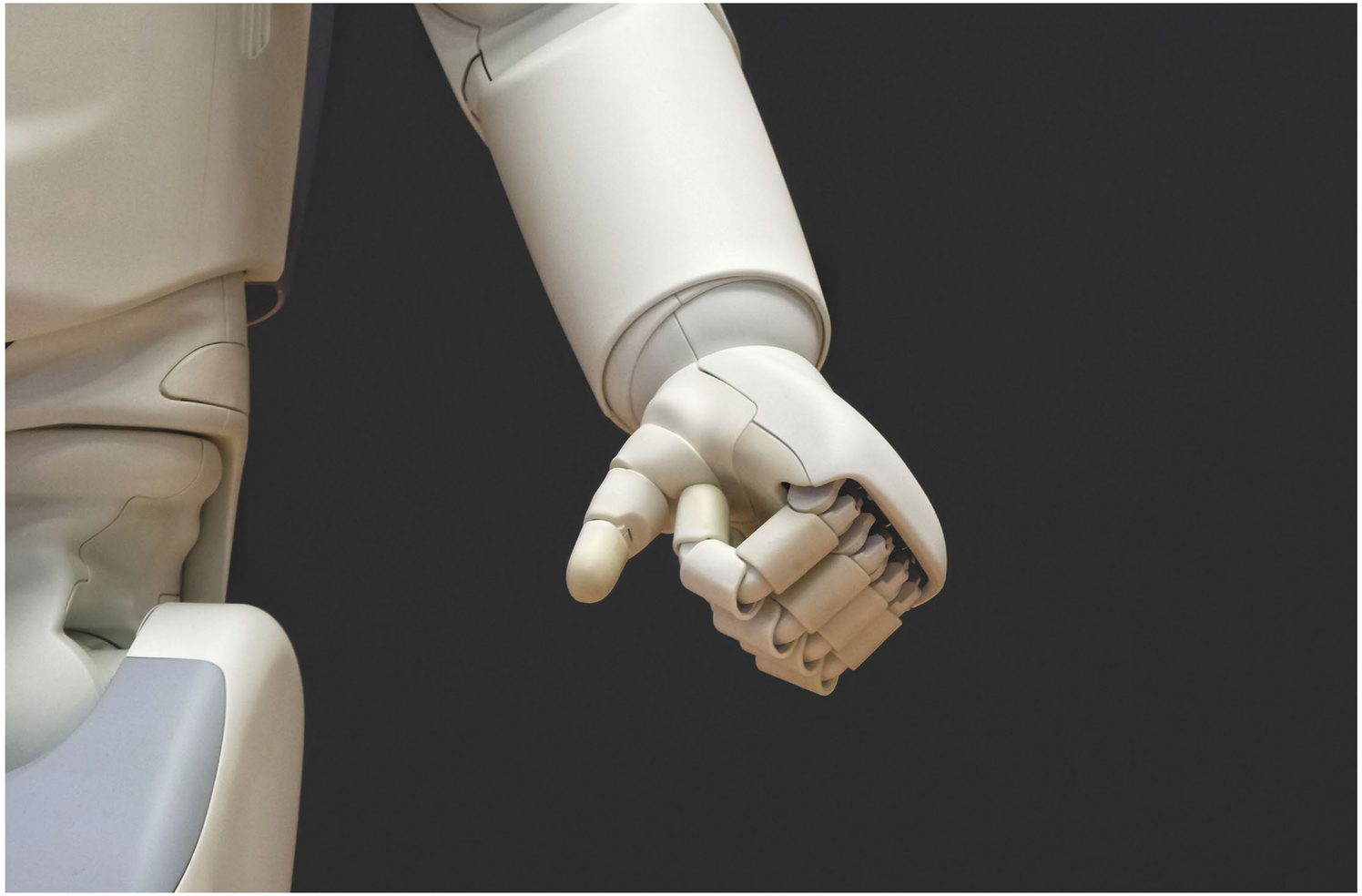
Australia

Regulation of AI

Liability regime for AI - 2/2

Next steps and relevance:

Considering the uncertainties around liability for AI products and services, this is an area that is likely to attract more attention in coming years. As AI products and services develop and become more complex, traditional liability regimes are likely to be challenged. Businesses should stay alert as to potential changes in this area.



China

AI as a digital asset: AI initiatives in China - 1/3

Latest developments:

On 12 August 2022, the Ministry of Science and Technology (MOST) and another five departments released the *Guidance on Accelerating Scene Innovation to Promote High-Level Application of Artificial Intelligence for High-Quality Economic Development* (the "Guidance), which clearly sets scene innovation as the development goal of both AI technology upgrades and new paths for industrial growth. The Guidance also puts forward specific measures including creating major scenes for AI, improving innovation capabilities for AI scenes, accelerating the opening of AI scenes, and strengthening the supply of innovation elements for AI scenes.

Following the Guidance, on 15 August 2022, the MOST issued the Notice on Supporting the Construction of *New Generation Artificial Intelligence Application Scenarios*, releasing the first batch of application scenarios with good foundations. The first batch of application scenarios involve 10 specific fields including smart farms, smart ports, smart mines, smart factories, smart homes, smart education, autonomous driving, smart diagnosis and treatment, smart courts, and smart supply chains.

Summary:

Categories of major AI scenarios

The Guidance proposes that one of the development goals of AI scenario innovation is to accelerate the emergence of major application scenarios in the fields of economic and social development, scientific research discoveries, and major activity guarantees. The Guidance divides major AI scenarios into 4 categories and encourages exploration of the application scenarios for AI technology in these scenarios:

- **Category 1.** Cultivation of a high-end, efficient and intelligent economy: an in-depth exploration of the application scenarios for AI technology in key industries such as manufacturing, agriculture, logistics, finance, commerce, and home furnishing shall be encouraged to promote the high-end and efficient development of the smart economy.
- **Category 2.** Construction of a safe, convenient, and intelligent society: opportunities in AI application scenarios shall be continuously explored in the fields of urban management, traffic management, ecological protection, medical health, education, and old-age care, with the goal of building a smarter city and more intimate society, and demonstration of intelligent social scenario application shall be carried out.

China

AI as a digital asset: AI initiatives in China - 2/3

- **Category 3.** High-level scientific research activities: Greater efforts shall be made to make AI technology become a new paradigm for solving major scientific problems in the fields of mathematics, chemistry, geosciences, materials, biology, and space science.

- **Category 4.** Major national events and major projects: the application scenarios of AI shall be expanded in major events and conferences such as the Asian Games, National Games, China International Import Expo, and China International Fair for Trade in Services, thus providing testing and verification opportunities for AI technology and product applications. The use of AI technology in major construction projects such as strategic backbone passages, high-speed railroads, port and shipping facilities, and modern airport construction shall be encouraged to improve the construction efficiency of major projects.

Supply of the elements of AI scenario innovation

In order to promote the development of AI scene innovation, the Guidance puts forward policy encouragement opinions from various aspects of elements supply:

- **Computing power facilities:** The opening and sharing of AI infrastructure resources such as computing power platforms, generic technology platforms, industry training data sets, and simulation training platforms shall be encouraged. Guidance also encourages local governments to reduce AI enterprises' cost of infrastructure use. New technologies such as blockchain and privacy computing are adopted to provide open data services for typical AI application scenarios on the basis of ensuring data security. The security protection of the "data base" shall be strengthened, and personal information, trade secrets, and important industry data shall be protected according to the law.

- **Data resources:** New technologies such as blockchain and privacy computing are adopted to provide open data services for typical AI application scenarios on the basis of ensuring data security.

- **Talents in scenario innovations:** Universities and vocational colleges are encouraged to cultivate professional talents with innovative awareness and ability of AI scenarios through professional curriculum setting, training exchanges and other forms.

- **Market resources:** Banking, insurance, and other financial institutions shall be encouraged to provide financial support. Large enterprises in the industry shall be encouraged to provide supply chain support for the implementation of scenario projects.

China

AI as a digital asset: AI initiatives in China -3/3

How could it be relevant for you?

For enterprises that develop and apply AI technology, the Guidance points out major application scenarios for AI, emphasises the importance of scenario innovation for the high-quality development of the national economy, and provides policy incentives for enterprises to carry out AI scenario innovation. In addition, it is recommended that enterprises keep a close eye on the legislative and enforcement developments of AI technology.

Next steps:

In recent years, the Chinese government has continuously increased its support for the innovative development and application of AI at the policy level, and the centre of AI-related policies has gradually shifted from strategic deployment to technological application, implementation and innovation.

Additionally, on 30 August 2022, the *Regulations of Shanghai Municipality on Promoting the Development of Artificial Intelligence Industry (Draft)* was released for public comments. The draft intends to promote the development of Shanghai's AI industry by improving the management mechanism, and optimising the allocation of computing power, algorithms, data and other elements of resources. On September 6, the first special local legislation for the AI industry - the Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations (the "Shenzhen AI Regulations) was officially announced and will come into effect on 1 November 2022. The Shenzhen AI Regulations create an innovative product access system. Low-risk AI products and services that do not have national or local standards but meet international advanced product standards or specifications are allowed to be tested and piloted. It is expected that other local governments in China will follow the example of Shanghai and Shenzhen to issue local policy or legislation to introduce more specific measures to promote the development of the AI industry.

Hong Kong

Guidance on Ethical Development and Use of AI - 1/2

Study on "Fostering Consumer Trust - Ethical AI in Hong Kong"

Latest developments:

Currently, there are no AI-specific laws or regulations in Hong Kong (except measures adopted to ban certain AI products involving personal safety such as autonomous driving AI). Local regulators have issued high-level guidance on AI and AI products, including *High-level Principles on AI* by the Hong Kong Monetary Authority, Guidelines on *Online Distribution and Advisory Platforms* by the SFC (both published in 2019) and the latest *Guidance on Ethical Development and Use of AI* (**AI Guidance)** by the PCPD in August 2021 for organisations to self-assess whether practices recommended in the AI Guidance have been adopted.

Summary:

Data Stewardship Values and Ethical Principles for AI

The AI Guidance recommends three fundamental Data Stewardship Values, namely, being respectful of the dignity, autonomy rights, interests and reasonable expectations of individuals; beneficial and fair to stakeholders when organisations develop and use AI. In line with international standards such as the European Commission's Proposal for Regulation of AI and UNESCO and OECD Recommendations on AI, the AI Guidance sets out the following seven ethical principles for AI:

- **Accountability:** Organisations should be accountable for what they do and be able to provide sound justifications for their actions;
- **Human Oversight:** Organisations should ensure that appropriate human oversight is in place for the operation of AI where AI system users should be informed and able to act autonomously with regards to recommendations or decisions of the AI systems;
- **Transparency and Interpretability:** Organisations should disclose their use of AI and relevant policies while striving to improve the interpretability (i.e. the ability to determine the cause and effect) of automated decisions and decisions made with the assistance of AI;
- **Data Privacy:** Effective data governance should be put in place to ensure proper handling and protection of personal data involved in the development and use of AI;
- **Fairness:** Organisations should avoid bias and discrimination in the use of AI – any differential treatment between different individuals (or groups of individuals) should be validly justifiable;
- **Beneficial AI:** Organisations should use AI in a manner that benefits and minimises harm to stakeholders; and
- **Reliability, Robustness and Security:** Organisations should ensure reliable operation of AI systems which are resilient to errors and guarded against attacks.

Hong Kong

Guidance on Ethical Development and Use of AI - 2/2

Study on “Fostering Consumer Trust - Ethical AI in Hong Kong”

Practice Guide

The set of practice guide within the AI Guidance provides practical examples of how organisations should approach AI governance when implementing AI in their operations, from inception to implementation and ongoing risk-based management, covering the following areas:

- AI strategy and governance;
- Risk assessment and human oversight;
- Development of AI models and management of overall AI Systems; and
- Communication and engagement with stakeholders.

How could it be relevant for you?

Organisations that intend to or have begun to develop and use AI technology in their operations are advised to assess the risk levels of their AI systems and the data privacy concerns involved and to implement the PCPD’s recommended best practices for better compliance with the relevant requirements of the Personal Data (Privacy) Ordinance.

Next steps:

With Hong Kong’s vision of becoming a regional data hub in innovation and technology and the increasing applications and use of AI technology in business, it is anticipated that there will be more robust AI development and governance in Hong Kong.

Hong Kong

Guidance on Ethical Development and Use of AI

Study on "Fostering Consumer Trust - Ethical AI in Hong Kong" - 1/2

Latest developments:

On 8 September 2022, the Consumer Council (the **Council)** published its first study on the use of AI in e-commerce in Hong Kong (the **Study)** with an aim to promote responsible and ethical AI in e-commerce, and possibly pave the way for a local AI governance framework.

Summary:

The Study focuses on business-to-consumer (B2C) e-commerce and is comprised of: (i) a quantitative online consumer survey; (ii) review of e-commerce platforms among local consumers; (iii) interviews with major e-commerce traders, technology providers and industry experts in Hong Kong; (iv) research on relevant guidelines and initiatives on the use of AI in 10 selected jurisdictions; and (v) review of consumer cases. The Council identified a number of key concerns as follows:

- AI is a double-edged sword to consumers whose confidence could be enhanced through effective risk mitigation (including human oversight);
- Consumers are unfamiliar with AI - they expect the right to know the risks they are facing and the right to choose whether to take the risks;
- Accuracy and stability of AI tools;
- A lack of, or inadequate, privacy policies of online stores that uses AI;
- Inadequate support for industry practitioners to tackle challenges in talents, funding and data relating to AI; and
- The lack of an integrated and holistic blueprint for local AI development and governance framework.

The Council recommended the following relevant to different stakeholders:

- Traders to adopt the checklist of best practices to formulate company AI policy and governance;
- Industry associations to establish a "Consumer Charter" to boost consumer confidence;
- Consumers to follow tips to be smart when shopping online;
- Government to nurture AI understanding of the public and traders; establish a holistic policy for AI development; and build a fair and competitive e-commerce market.

Hong Kong

Guidance on Ethical Development and Use of AI

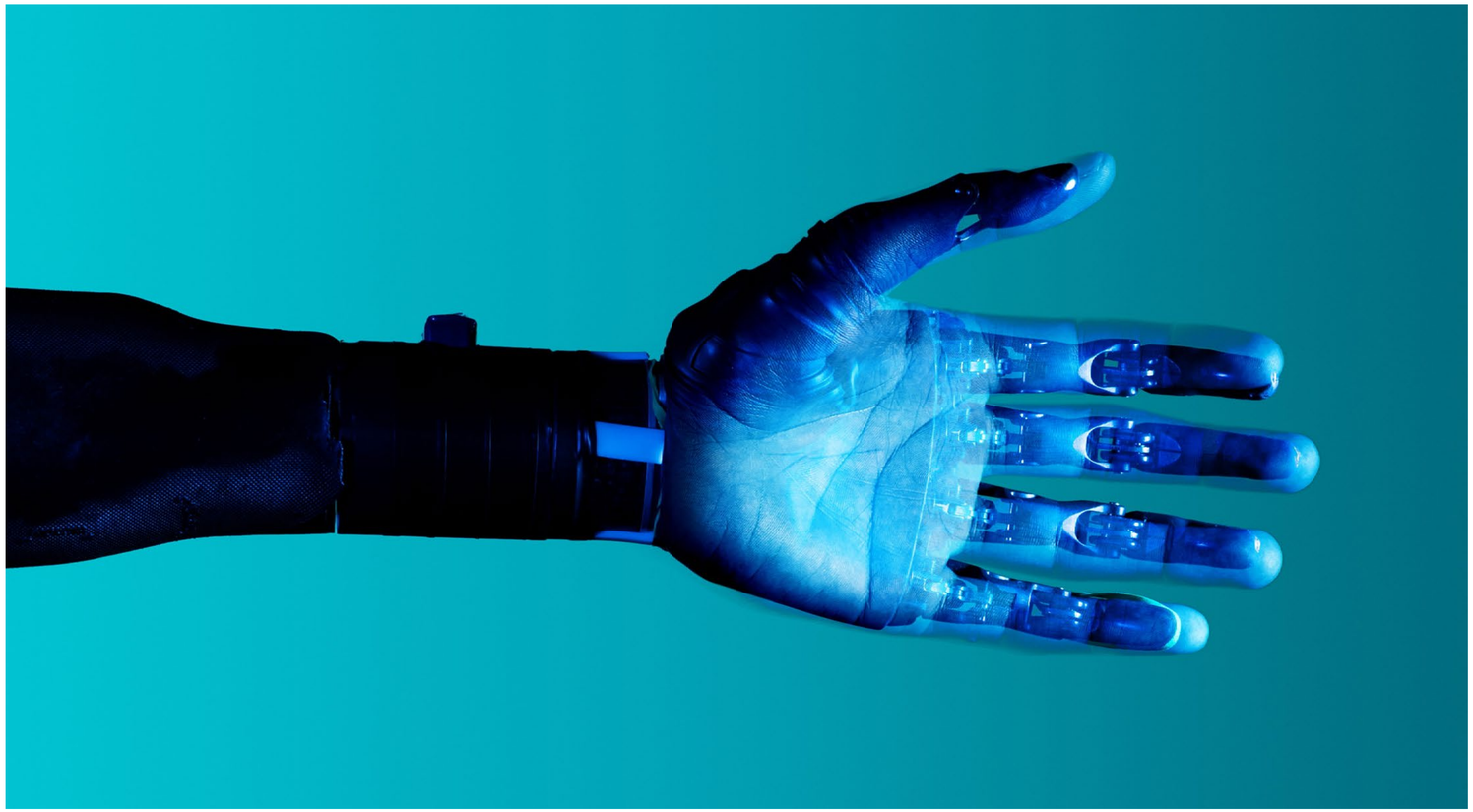
Study on “Fostering Consumer Trust - Ethical AI in Hong Kong” - 2/2

How could it be relevant for you?

The Study identified the urgent need for e-commerce traders to adopt good trade practices when using AI. Operators of e-commerce platforms should also review their respective privacy policies. Trade associations could also consider establishing a “Consumer Charter” for traders to follow, hence protecting consumers.

Next steps:

The Hong Kong Government is actively promoting digital transformation and AI development. In line with the increasing international regulatory momentum on AI, the Study recommended that Hong Kong can reference the experiences and approaches of other jurisdictions and expedite the development of a cross-sectoral approach to regulate AI in Hong Kong.



Singapore

AI Governance Testing Framework and Toolkit – 1/2

Latest developments:

On 25 May 2022, the IMDA and PDPC launched "AI Verify", the world's first AI governance testing framework and toolkit. AI Verify is intended for voluntary adoption by companies to self-test their AI systems against a set of ethical principles, and to provide companies with a means to demonstrate responsible implementation of AI to their stakeholders in an objective and verifiable way.

AI Verify is the latest in a series of AI governance initiatives taken Singapore in recent years. In contrast to the approach in Europe which has proposed legislation to introduce an AI legal and regulatory framework, the approach in Singapore so far remains centered around the issuance of voluntary frameworks and best-practice guidance, such as the Singapore Model AI Governance Framework (now in its 2nd edition).

Summary:

The AI Verify testing framework and toolkit is based on the following 8 AI ethics principles, which were selected by the IMDA and PDPC following a survey of internationally accepted AI ethics principles:

- Transparency (appropriate information is provided to individuals impacted by AI systems);
- Explainability (ability for users to understand and interpret what AI systems is doing);
- Repeatability/Reproducibility (AI results consistent);
- Safety (impact/risk assessment conducted and known risks identified/mitigated);
- Robustness (AI systems can still function despite unexpected inputs);
- Fairness (no unintended bias, data used to train models is representative);
- Accountability (proper management oversight of AI systems development); and
- Human Agency and Oversight (AI systems designed in a way that they will not decrease human ability to make decisions).

AI Verify comprises two main components:

- The **testing framework** which sets out definitions of each of the AI ethics principles, testable criteria that combine technical and non-technical factors, testing processes (actionable steps to ascertain if the testable criteria are met), and metrics; and

AI as a digital asset

Singapore

AI Governance Testing Framework and Toolkit - 2/2

- The **toolkit** which covers technical tests and process checks described in the testing framework. The toolkit provides a user interface to guide users step-by-step in the testing process, and produces a basic summary report to enable system developers and owners to interpret test results.

How could it be relevant for you?

Companies that are interested in getting early access to the AI Governance Testing Framework and Toolkit to conduct self-testing on their AI systems and models can contact the IMDA and PDPC to express their interest to participate in the pilot. In addition to getting early access, pilot participants will have the opportunity to produce test reports to demonstrate transparency and build trust with stakeholders, and to provide feedback to help shape future versions of the framework and toolkit.

Next steps:

AI Verify is currently in its pilot phase. Feedback provided by industry participants in the pilot will be used to enhance the testing framework and toolkit, with the aim of releasing an updated framework and toolkit version at the end of the pilot.

Privacy & Data Protection

CHAPTER 4

Australia

Latest developments:

Australian privacy law is currently undergoing a period of change. In December 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (**OP Act**) came into effect, giving the OAIC further powers and increasing the penalties for serious data breaches. Further, in February 2023, the Commonwealth Attorney-General released the Privacy Act Review Report (the **Report**) proposing a range of further changes to the Privacy Act. These changes and proposals have been accelerated by a series of high-profile data breaches suffered by Australian companies in late 2022, which have increase public pressure on the Federal Government to strengthen Australian privacy law.

Australia

Privacy Act Reform

Attorney-General's Report - 1/2

Privacy Legislation Amendment Act 2022

Consumer Data Right Privacy Act Reform

Summary:

The Report sets out a wider tranche of proposed reforms which, if passed, will affect all organisations that are subject to the Privacy Act, including the following:

- The introduction of a controller/processor distinction;
- Broadening the definition of 'personal information', to include information 'relating to' an individual as opposed to just 'about' an individual;
- Eventually removing the small business exemption but only after steps have been implemented to assess the impact of this change and facilitate compliance;
- In the shorter term, making the collection of biometric information for use in facial recognition technology an exception to the small business exemption and also removing the consent exception for small businesses that trade in personal information;
- Further consultation regarding the implementation of enhanced privacy protections for private sector employees;
- Changes to the political and journalism exemptions;
- A requirement that any collection, use and disclosure of personal information be fair and reasonable in the circumstances;
- The introduction of a statutory tort for a serious invasion of privacy;
- The introduction of a direct right of action in relation to an interference with privacy;
- A requirement to notify the Office of the Australian Information Commissioner of eligible data breaches within 72 hours, as opposed to 30 days;
- The introduction of standard contractual clauses for use when transferring personal information overseas;
- A requirement to include various additional matters in APP entities' privacy policies and collection notices;
- Obligations in relation to de-identified information, for example a requirement that APP entities take reasonable steps to protect de-identified information and prohibitions on re-identification;
- Enhanced individual rights (though subject to exceptions), including:
  - A right to erasure;
  - Broader access and correction rights;
  - A right to object to the collection, use or disclosure of personal information;
  - A right to de-index certain online search results; and
  - An unqualified right to opt-out of the use or disclosure of personal information for direct marketing or targeted advertising purposes;

Australia

- As well as an obligation on APP entities to provide reasonable assistance to individuals in respect of such rights;
- Obligations to undertake privacy impact assessments for activities with high privacy risks;
- A requirement to determine and record purposes for the collection, use and disclosure of personal information at the time

How could it be relevant for you (if passed)?

If the proposals above are brought into law, it is likely that most organisations will need to review their privacy practices and documentation to ensure compliance with the Privacy Act as amended.

Next steps:

The Report signposts significant changes to Australia's privacy laws and it is possible we will see draft legislation as early as the second half of 2023. Entities who do business in Australia should review their current privacy practices and consider which proposals might require system or other process improvements.

Summary:

Following a series of high-profile data breaches suffered by Australian entities which left millions of Australians' personal information vulnerable to hackers, the Federal Government passed the *Privacy Legislation Amendment (Enforcement and Other Measures) Act* 2022 in December 2022. This Act comprised three main changes in respect of privacy regulation, namely:

- Increasing the maximum penalty for serious or repeated interferences with privacy for body corporates from $2.2 million to the greater of $50 million, three times the value of the benefit obtained attributable to the breach or, if the court cannot determine the value of the benefit, 30% of the entity's adjusted turnover during the breach turnover period for the contravention;
- Enhancing the OAIC's information gathering and sharing powers, particularly following a data breach; and
- Extending the jurisdiction of the Privacy Act to capture businesses that 'carry on business in Australia', even if they do not collect or hold information in Australia.

How could it be relevant for you?

Businesses that handle personal information now have a greater incentive to ensure that they are compliant with the Privacy Act, given the hefty increase in potential penalties in the event of a breach. Businesses should also be wary of the potential changes to the Privacy Act which may arrive in 2023, as they may vary or impose new obligations on organisations that handle personal information.

Next steps:

The Federal Government has signalled that the above amendment is the first in what it is expecting to be a series of wide-ranging reforms to the Privacy Act. It is anticipated that a draft bill which revamps the wider Privacy Act will be tabled in Parliament in 2023.

Latest developments:

In November 2021, the federal government registered the rules which expand the consumer data right (**CDR**) to the energy sector, which has been operational in the banking sector since July 2020. The rollout to the energy sector is the second step in an economy-wide rollout. The CDR now applies to the Australian Energy Market Operator, AGL Energy Group, Origin Energy Group and Energy Australia Group.

In January 2022, the federal government formally expanded the CDR regime to the telecommunications and open finance sectors. The treasury, with the support of the new Albanese Government, proposed further expansions to CDR provisions contained in consumer laws as set out in the exposure draft of the *Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation*.

Summary:

The focus of the CDR is data portability. It was brought in to provide consumers a right to directly access specified data held by certain businesses about themselves. It also empowers these customers to direct certain providers of products or services to safely share such data with accredited third parties.

Businesses subject to the CDR must also comply with the 13 privacy safeguards, which are designed to protect the personal information of consumers.

The *Treasury Laws Amendment (Measures for Consultation) Bill 2022: Consumer Data Right – Implementing Action Initiation* exposure draft proposes to introduce two new CDR accreditations:

- Accredited Action Initiator (AAI) – an accredited entity that is able to instruct Action Service Providers on a consumer's behalf; and
- Action Service Provider (ASP) – an entity that carries out instructions received from an AAI.

These new accreditations will expand the ability of third parties to initiate CDR actions on behalf of a consumer beyond their current consent based data sharing processes.

Consultations on the Bill closed on 24 October 2022.

The new Bill would enable the Government to progress plans to implement an overall transition to an economy wide roll out of the CDR.

How could it be relevant for you?

Businesses in the banking, energy, telecommunications, and open finance sectors should be aware of the CDR obligations set to be imposed on them at a later date and will need to assess, ahead of the CDR's rollout to their sectors, whether any changes should be made to their data arrangements and business systems in order to be able comply with such obligations in future.

Next steps:

In March 2022, the Treasury released design papers on the application of the CDR in the telecommunications and open finance sectors. Feedback from these consultation processes will likely inform the development of the CDR obligations for these sectors. Further developments on the roll-out are expected in 2023.

China

Privacy and data protection: the latest developments on cross-border data transfer

Latest developments:

On 1 September 2022, the *Measures of Security Assessment for Data Export* (**Measures**) which was released by the CAC on 7 July 2022 took effect, indicating that the security assessment regime set out by the *Cybersecurity Law* (**CSL**), the *Data Security Law* (**DSL**) and the PIPL has been established.

Summary:

Under the Measures, the Security Assessment applies to "export by the data processors of important data and personal information that is collected and generated in the course of operations in the territory of China". Apparently, export of important data and personal information collected or generated outside of China will be out of the scope. But the remote access from a foreign jurisdiction is considered as an export of personal information (**PI**) to that jurisdiction.

The Measures also lay down detailed scenarios where the Security Assessment applies to data export, which include:

- Export of important data;
- Export of personal information by critical information infrastructure (**CII**) operators;
- Export of personal information by a data processor that processes personal information of 1,000,000 individuals or more;
- Export of personal information by a data processor that from 1 January of last calendar year in aggregate exports (i) personal information of over 100,000 individuals or (ii) sensitive personal information of over 10,000 individuals; and
- Such other circumstances as designated by the CAC.

Before applying for the Security Assessment, the data processors must first conduct a self-assessment. The Measures set out the key contents of the self-assessment, including:

- The legality, legitimacy and necessity of the data export and the purpose, scope and means of the data processing by overseas recipients;
- The scale, scope, types, and sensitivity of the data to be exported and any risks of the export to national security, public interest, and legal interests of individuals or organisations;
- Whether the undertakings and the corresponding management and technical measures and capability of the overseas recipient will ensure safety of the data export;

China

Privacy and data protection: the latest developments on cross-border data transfer

Security Assessment - 2/3

Standard Contract

Certification

- The risks of unauthorised alteration, destruction, leak, loss, transfer or illegal acquisition or use of the data during and after the export, and the effectiveness of the channels for individuals to exercise their individual rights to the personal information; and
- Whether the contract or other documents of equivalent legal effect to be entered into between the overseas recipient and data processors have adequately provided for the data security protection obligations.

Where the Security Assessment is required, the data processor must submit the following materials, including:

- An application letter, the form of which is not specified and should be a standard one to be published by the CAC;
- A report on the self-assessment of data export risks;
- The legal document that the data processor and the overseas recipients propose to enter into; and
- Other materials as required by the authorities.

The Security Assessment will focus on the following aspects of the data export to evaluate the risks to national security, public interest and legal interests of individuals and organisations:

- The legality, legitimacy and necessity of the purpose, scope and means of the data export;
- The impact of the data security protection laws and policies and cybersecurity environment of the nation or region of the overseas recipient's domicile on data transfer security and whether the level of data protection of the overseas recipient meets the requirements of the laws, regulations and mandatory national standards of China;
- The scale, scope, types and sensitivity of the exported data and the risks of unauthorised alteration, destruction, leak, loss, transfer or illegal acquisition or use of the data during and after the export;
- Whether data security and personal information rights are adequately protected;
- Whether the Legal Document to be entered into between the overseas recipients and data processors has adequately provided for data security protection responsibilities and obligations;
- Compliance with Chinese laws, regulations and ministerial rules; and
- Other items that the CAC considers necessary.

The data processors must submit the application to the CAC of provincial level, which will have 5 working days to review completeness of application materials before passing the application on to the central CAC.

The central CAC is required to complete the security assessment within 45 working days of accepting the application and has the power to extend the time period in complicated cases or where supplemental or corrected materials need to be provided, after notifying the applicants of the extended period. The data processors will be notified in writing of the assessment result, which will be valid for two years from the date of the issuance of the result and the whole process could take 57 working days or more.

China

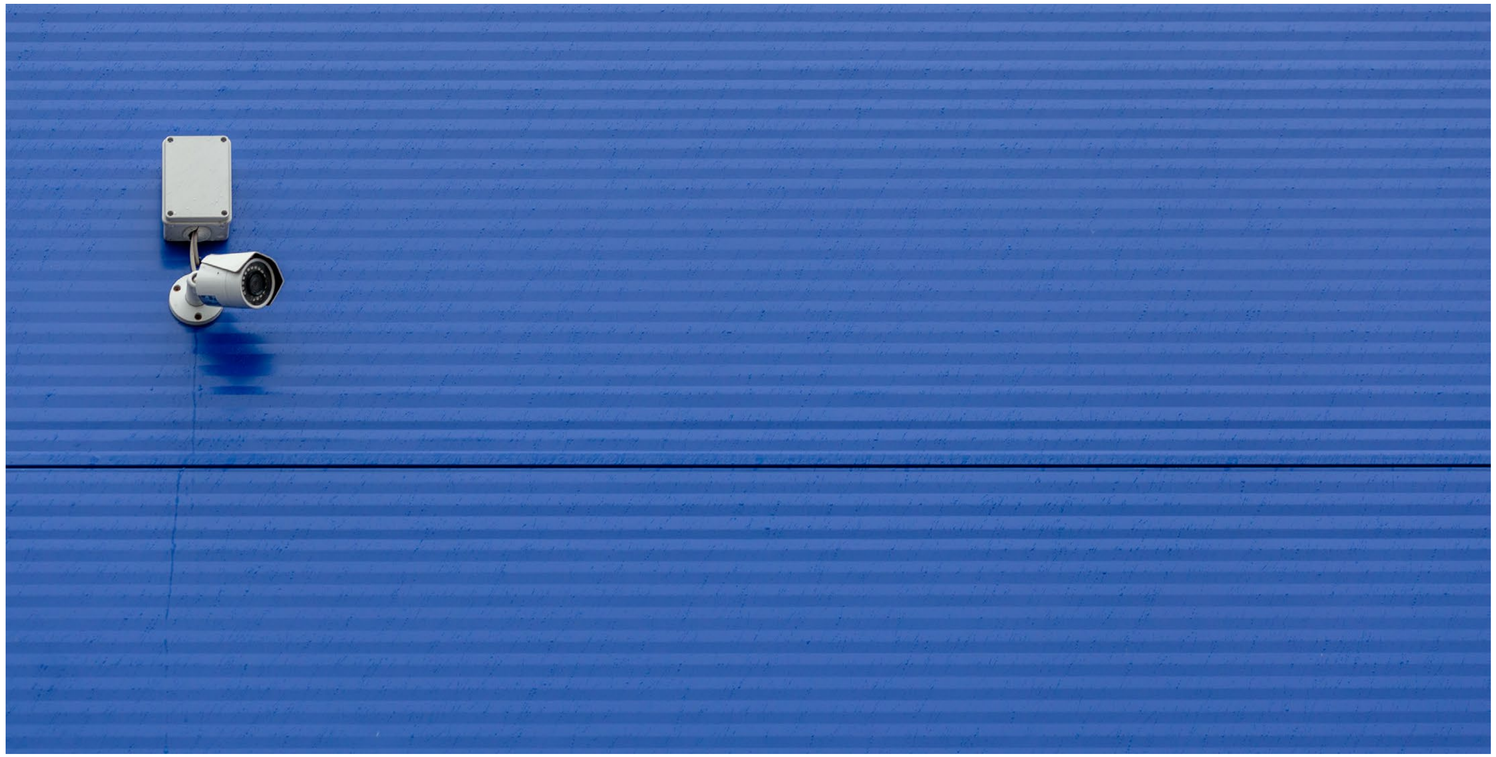
Privacy and data protection: the latest developments on cross-border data transfer

How could it be relevant for you?

Where the export activities fall into the scenarios where a security assessment is required, data exporters have to apply for the security assessment and get the assessment approval, or they may be fined by the regulators according to the CSL, the DSL and the PIPL, which could be up to the higher of 50 billion CNY or 5% of last year's turnover. Considering the short grace period, the data processors affected by the Measures should take immediate actions to ensure compliance.

Next steps:

The CAC has released the Guidelines on the Application for Security Assessment for Data Export and several provincial CAC (incl. Beijing, Tianjin, Hebei, Shanghai, Jiangsu and Zhejiang) have provided contact detail for consultation. It is expected that more law enforcement actions will emerge since the 6-month grace period has passed.



China

Privacy and data protection: the latest developments on cross-border data transfer

Latest developments:

On 24 February 2023, the CAC released a draft of the long-awaited finalised standard contract for personal information export and an accompanying regulation (**Standard Contract Regulation**) for public consultation, providing us a preview of the standard contract regime set out by Article 38 of the PIPL.

Summary:

Under the PIPL, the PI processor (i.e. the counterpart concept of the data controller under the GDPR) may consider using the Standard Contract as its route for exporting PI, only if the proposed export is not subject to the Security Assessment that applies to the following scenarios:

- Export of important data;
- Export of personal information by CII operators;
- Export of personal information by a data processor that processes personal information of 1,000,000 individuals or more;
- Export of personal information by a data processor that from 1 January of last calendar year in aggregate exports (i) personal information of over 100,000 individuals or (ii) sensitive personal information of over 10,000 individuals;
- Such other circumstances as designated by the CAC.

The Standard Contract Regulation refers to the exporter as the "**PI processor**", which is in line with the PIPL. Apparently, neither the PIPL nor the Standard Contract Regulation contemplates that the restrictions on data export will apply to exporters who are entrusted by the PI processor with processing PI (**Entrusted Parties**). The Standard Contract does not differentiate the role of the data importer as a PI processor or an entrusted party. In summary, a data exporter that is a PI processor may use the Standard Contract to export personal information to a data importer that is either a PI processor or an Entrusted Party.

The Standard Contract Regulation requires a PI processor to conduct a PIPIA and further provides for key aspects that a PIPIA for data export must cover, including the assessment of the impact of the PI protection policies, laws and regulations of the country or region where the data importer is located upon the performance of the Standard Contract.

The Standard Contract Regulation also requires PI processors to file with the local provincial CAC within 10 working days from the effective date of the standard contract and submit the standard contract and the PIPIA report.

China

Privacy and data protection: the latest developments on cross-border data transfer

In the Standard Contract, the data exporters must notify the individuals that they have been made third-party beneficiaries unless they expressly refuse within 30 days of being notified. The data exporters will now need to make sure that they have included in the privacy notice content on third-party beneficiaries and contact details, via which the individuals express their objection. In addition, as third-party beneficiaries, individuals are given the rights to enforce the obligations of the data exporters and importers under the Standard Contract.

Next steps and relevance:

The finalised Standard Contract and the relevant regulation marks that China has established mechanism for exporting PI via Standard Contract.

Compared with Security Assessment and Certification (see below), the Standard Contract would be the most convenient and commonly used route for exporting PI. Whilst the Standard Contract of China bears many similarities with the SCCs under the GDPR, the data importers and exporters should pay attention to the worth-noting differences and consider its compatibility with the current cross-border transfer tools.

China

Privacy and data protection: the latest developments on cross-border data transfer

Latest developments:

On 16 December 2022, the National Information Security Standardisation Technical Committee (**TC260**) circulated the 2.0 version of the *Technical Certification Specification for Certification of Personal Information Cross-border Processing* (Certification Specification 2.0).

Summary:

The Certification Specification explicitly requires PI processors, who will apply for the certification, to comply with the requirements of the non-binding national standards *Information Security Technology – Personal Information Security Specification* published by the TC260 (Security Specification).

The Certification Specification 2.0 provides for who are qualified to apply for the PI Export Certification:

- The entities located in China may apply for the certification with regard to the sharing within a multinational company or an economic or public entity.
- The local representatives established or designated by overseas PI Processors may submit the application on behalf of the foreign PI Processors. Pursuant to the PIPL, a foreign PI processor subject to the extraterritorial effect must establish or appoint a local representative in China.

The basic requirements under the Certification Specification include:

- Legally binding and enforceable documents: Relevant parties involved in cross-border processing of personal information should sign legally binding and enforceable documents to protect the rights of individuals.
- Organisational management: Both the PI processor (i.e. the exporter) and the overseas recipient involved in cross-border processing activities should designate their own personal information protection officers and establish their personal information protection departments to carry out certain data protection tasks in the cross-border processing activities
- Unified cross-border processing rules: The PI processor (i.e. the exporter) and the overseas recipient must abide by a set of unified cross-border processing rules, which should at least include the following contents:
  - Details of cross-border processing, including volume, scale, categories and sensitivity of personal information;

China

Privacy and data protection: the latest developments on cross-border data transfer

Security Assessment

Standard Contract

Certification - 2/2

- The purposes, means and scope of cross-border processing;
- Retention period and disposal methods upon expiry of the period;
- Countries or regions where personal information will be transferred in transit;
- Resources and measures that are required for protecting rights of individuals; and
- Compensation and response plans related to personal information security incidents.

- PIPIA: The PI processor (i.e. the exporter) should conduct a PIPIA prior to exporting personal information outside of China.

How could it be relevant for you?

Some essential elements of the certification regime are not addressed by the Certification Specification, such as the accredited certification bodies, the certification procedure and the effective period of the certification, which we expect to be covered by future regulations and guidelines. As such, a more practical option for companies to export PI at this stage is to opt for Standard Contract if companies will not be subject to the Security Assessment.

Next steps and relevance:

The Certification Specification 2.0 is a useful attempt of the TC260 towards establishing the certification regime for data export in China, but the regime will not be completed in the absence of higher-level mandatory regulations. In addition, many questions like how the Certification Specification applies to PI processor subject to the extraterritorial effect of the PIPL need to be further explained.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing - 1/4

New Guidance on Cross-border transfer of Personal Data

Latest developments:

On 8 October 2021, the Personal Data (Privacy) (Amendment) Ordinance 2021 (the **Amendment Ordinance)** came into effect to combat malicious doxxing acts so as to protect personal data privacy of individuals.

Summary:

The Amendment Ordinance amends the PDPO by introducing anti-doxxing provisions which can be categorized as follows:

(i) Creating offences to curb doxxing acts committed without the data subject's consent

There are a total of seven (7) new offences: two-tier offences on doxxing with five (5) ancillary offences related to non-compliance with or obstruction of investigative and enforcement powers exercised by the Privacy Commissioner of Personal Data (PCPD).

The two-tier doxxing offences are as follows:

- **First tier offence:** Section 64(3A) makes it an offence for any disclosure of personal data of a data subject without the relevant consent of the data subject (a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or (b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.

- **Second tier offence:** This is provided under Section 64(3C) which is similar to Section 64(3A), save that the offence relates to whether disclosure *causes any specified harm* to the data subject or any family member of the data subject.

  "Specified harm" in relation to the two-tier offences means (a) harassment, molestation, pestering, threat or intimidation to the person; (b) bodily harm or psychological harm to the person; (c) harm causing the person reasonably to be concerned for the person's safety or well-being; or (d) damage to the property of the person.

- A person who commits a first tier offence is liable on summary conviction to a level 6 fine (i.e. HK$100,000) and imprisonment for 2 years; while a person who commits a second tier offence is liable for conviction on indictment to a fine of HK$1,000,000 and imprisonment for 5 years.

The five (5) ancillary offences relate to non-compliance with or obstruction of investigative and enforcement powers of the PCPD (as further discussed in (ii) and (iii) below) are as follows:

- Non-compliance with a notice;
- Non-compliance with a notice with intent to defraud;
- Obstruction, hindrance or resistance to investigations;
- Non-compliance with a cessation notice; and
- Non-compliance with secrecy obligations.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing - 2/4

New Guidance on Cross-border transfer of Personal Data

(ii) Empowering the Privacy Commissioner to carry out criminal investigation and institute prosecution

The new PDPO empowers the PCPD with four (4) main types of prosecution and investigative powers:

- **Power to prosecute offences:** Such powers cover not just the proposed new doxxing offence, but other criminal offences in the PDPO. The enhanced power does not derogate from the powers of the Secretary of Justice to prosecute criminal offences.
- **Power to require delivery of materials and provide assistance:** Such powers include, among others, the power to require a person to provide the PCPD with materials, require a person to answer questions or require a person to give the PCPD all the assistance reasonably required.
- **Power in relation to premises and electronic devices:** Such power includes, among others, search and seizure powers (with warrant) at relevant premises and access of electronic devices (with or without warrant) to assist with investigations.
- **Power to stop, search and arrest persons:** Such powers may be exercised, without warrant, by the PCPD (or a person authorised by the PCPD) to stop, search and arrest any person reasonably suspected of having committed a doxxing or related offence.

(iii) Conferring on the Privacy Commissioner statutory powers to demand the cessation of doxxing contents

In addition to the powers set out in (ii) above, if the PCPD has reasonable ground to believe that (a) there is a subject message; and (b) a "Hong Kong person" is able to take a cessation action (whether or not in Hong Kong) in relation to the message, then the PCPD may serve a "cessation notice" on the person directing the person to take the cessation action.

"Cessation action" includes removing the message from the electronic platform, ceasing or restricting access by any person of the platform or discontinuing the hosting service for the platform.

It is worth noting the extra-territorial scope of the proposed "cessation notice" regime. So long as:

- The relevant message concerns a disclosure (whether taking place inside or outside Hong Kong) of a Hong Kong resident or a person that is present in Hong Kong (at the time when the disclosure is made), and the person that discloses the personal data essentially commits the doxxing offence described above; and
- The person that is going to receive the cessation notice can take the cessation action, a cessation notice can be issued, regardless of where the recipient of the notice is located.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing - 3/4

New Guidance on Cross-border transfer of Personal Data

Enforcement actions

Since the Amendment Ordinance came into effect in October 2021, the PCPD has been relatively active in taking enforcement actions against suspected doxxing offences.

The first arrest took place in May 2022. A person was suspected of having disclosed the personal data, including the mobile phone number, occupation, residential address and names of their employers without consent, on a social media platform in October 2021, amid a money dispute. The defendant was arrested on 13 December 2021 and was charged with four charges of disclosing personal data without consent with an intent to cause specified harm to the data subject or being reckless as to whether specified harm would be caused to the data subject under section 64(3A) of the PDPO. The case had its first mention on 25 May 2022, and we are at the date of this publication, not aware of any penalties that have been imposed.

Separately, the first conviction under the new anti-doxxing regime took place on 6 October 2022. This was the fourth arrest made by the PCPD, whereby the defendant disclosed on four social media platforms the complainant's personal data, including her name, photos, residential address, private and office telephone numbers, name of her employer and position without her consent, in contravention of section 64(3A) of the PDPO. The defendant also impersonated the complainant to open accounts on three of the said platforms, and stated in the relevant messages that the complainant welcomed others to visit her at her address. Many strangers later contacted the complainant and tried to get acquainted with her. A total of seven charges were laid against the defendant in respect of the doxxing offence and the defendant pleaded guilty to and was convicted of all seven charges and was sentenced to an 8 months' imprisonment.

The second sentencing case prosecuted by PCPD concluded on 8 March 2023. The defendant was an online trader and the victim was her supplier. Their business relationship turned sour because of a monetary dispute. The defendant then in December 2021 disclosed in 14 groups on a social media platform (1) allegations about the victim's fraudulent behaviour; and (2) personal data such as the Chinese names and photos of the victim and her husband, and the phone number of the victim. The PCPD arrested the defendant on 26 July 2022. The defendant pleaded guilty to all charges and was convicted by the Court on 1 February 2023. The conviction relates to the defendant's disclosure of the personal data of the victim and her husband without their consent, with an intent to cause specified harm to them or their family members, or being reckless as to whether specified harm would be (or would likely be) caused to them or their family members, in contravention of section 64(3A) of the PDPO. Based on the relevant reports and the nature of this case, the court sentenced the defendant to two months of imprisonment, suspended for two years.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing - 4/4

New Guidance on Cross-border transfer of Personal Data

How could it be relevant for you?

With the advancement of technology, doxxing contents can be spread and reposted in a click. To remove doxxing contents in an expeditious manner, in relation to a message, whether in written or electronic form, including but not limited to those posted on online platforms, a cessation notice may be served by the PCPD on Hong Kong service providers as well as non-Hong Kong service providers.

Further, as noted above, the PCPD is empowered to carry out investigations and request information and assistance in case of suspected doxxing offences. If you operate an online platform that processes personal data, you should be prepared for circumstances when your users may be suspected of committing relevant doxxing offences, and how to respond to cessation notices and other requests for information or assistance from the PCPD.

Next steps:

The Amendment Ordinance follows the last major amendment to the PDPO in 2013 when the PDPO introduced significant changes to the direct marketing regime in Hong Kong. According to the Report on the Work of the Office of the Privacy Commissioner for Personal Data in 2022 published for the meeting of the Legislative Council Panel on Constitutional Affairs on 20 February 2023, it is expected that the PDPO will be amended further in the near future to address other proposed amendments that were previously discussed in the legislature. A brief overview of some of the further proposed amendments to the PDPO is set out as follows:

- **Mandatory data breach notification:** Hong Kong currently does not require mandatory notification in the event of data breaches and it is expected that the PDPO may be amended to introduce mandatory data breach notifications in specified circumstances.
- **Regulation of data processors:** The PDPO currently does not directly regulate data processors and it is expected that the PDPO may be amended to directly bind data processors in certain instances e.g. in relation to data retention and security requirements, or notification requirements to the PCPD.
- **Data retention period:** It is expected that the PDPO will introduce express requirement on data users to specifically set out the retention periods for separate categories of personal data so that data subjects are clearly informed of the details of the retention policy.
- **Sanctioning powers:** The PCPD's power is expected to be further broadened by enabling the PCPD to impose administrative fines (linked to the annual turnover of the data user concerned) based on breaches of the requirements under the PDPO.

The Hong Kong Government and the PCPD's aim is to consult the Legislative Council Panel on Constitutional Affairs of the specific legislative proposals stated above concerning the Ordinance in the second quarter of 2023.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing

New Guidance on Cross-border transfer of Personal Data - 1/3

Latest developments:

On 12 May 2022, the PCPD issued a Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (the **"New Guidance)** which supplements the Guidance on Personal Data Protection in Cross-border Data Transfer issued in December 2014, introducing two sets of recommended model clauses (**RMCs)** to cater for the scenarios of cross-border data transfers between (i) "data user and data user" and (ii) "data user and data processor", respectively.

Summary:

The PDPO currently does not mandate model contractual clauses in the context of cross border data transfers. While Section 33 of the PDPO aims to regulate cross-border transfers of personal data from within Hong Kong to outside of Hong Kong, this section is not yet effective, and there is as yet no official timetable for implementation of this section.

Nevertheless, the New Guidance recommends and advises data users in Hong Kong to adopt the RMCs as part of their data governance responsibility to protect and respect the personal data privacy of data subjects. Hence, the adoption of the RMCs in commercial agreements between data transferors in Hong Kong and data transferees outside of Hong Kong is considered currently considered best practice rather than a mandatory obligation.

The RMCs for the two cross-border data transfer scenarios can be summarised as follows:

	Data user to another data user	Data user to data processor
Use/processing of data	The transferee will only use the personal data for the purposes of transfer agreed with the transferor (or directly related purposes).	Transferee will only process personal data for the purposes designated by the transferor.
Data is adequate but not excessive	The transferee will ensure that personal data transferred be adequate but not excessive for the purpose of transfer.	
Security	The transferee should apply agreed security measures to the use or processing of the personal data.	

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing

New Guidance on Cross-border transfer of Personal Data - 2/3

	Data user to another data user	Data user to data processor
Retention and erasure	The transferee will retain the personal data only for a period which is necessary for the fulfilment of the purposes of transfer and take all practicable steps to erase the personal data once the purposes of transfer have been achieved.	
Onward transfer	A transferee will not make any onward transfer of the personal data except as agreed by the parties; and should ensure that onward transfers of the personal data meet the requirements of the applicable RMCs.	
Access and correction rights of data subjects	Each party will comply with its obligation as a data user in respect of the access and correction rights of the data subject.	–

The RMCs set out in the New Guidance have been prepared as free-standing clauses, which may be incorporated into wider commercial agreements between data transferors and data transferees. Unlike the Standard Contractual Clauses promulgated by the European Commission (**EU SCCs)**, alternative wordings may be used to the extent the substance is consistent with the requirements of the PDPO. Specifically, the New Guidance advises data users to consider incorporating additional provisions, including:

- Additional contractual assurances, rights and obligations in relation to the use or processing of personal data in the context of each specific cross-border data transfer, in particular if the subject matter of the contract consists of more complex contractual obligations that last for a comparatively long period of time;
- Additional contractual assurances including, for example, (i) reporting, audit and inspection rights; (ii) notification of breach and (iii) compliance support and co-operation;
- In the context of data user-to-data user transfers, provisions relating to sharing personal data for direct marketing purposes and to contractual arrangements setting out agreed roles and responsibilities between the parties to ensure adequate protection be given to the personal data as provided under the PDPO.

The New Guidance specifically provides that the use of RMCs contributes to fulfilling the "Due Diligence Requirement" under Section 33(2)(f) of the PDPO for cross-border transfers, where data users can demonstrate they have taken reasonable precautions and exercised due diligence to ensure that the data will, in the jurisdiction of the transferee, be collected, held, processed or used in a way that complies with the PDPO and that the data users have taken into account of the Data Protection Principles under the PDPO (**DPP)** under the PDPO. However, it should be noted that the RMCs should not be taken as fulfilling requirements of the General Data Protection Regulation of the European Union (**GDPR)** or be considered as an alternative to the EU SCCs, when any transfers outside of the EU that are controlled by a Hong Kong data user.

Hong Kong

Recent amendments to Personal Data (Privacy) Ordinance (PDPO) regarding anti-doxxing

New Guidance on Cross-border transfer of Personal Data - 3/3

How could it be relevant for you?

In the context of globalisation and digitalisation of the world economy, data protection laws around the world are adopting more sophisticated cross border transfer regimes to ensure adequate protection of personal data. It is interesting to note that the New Guidance in particular seeks to clarify the scope of application of Section 33 of the PDPO to not only cover cross-border transfers of personal data from a Hong Kong data user to an entity outside Hong Kong, but also data transfers between two entities outside Hong Kong, as long as such transfer is controlled by a data user in Hong Kong.

If you are engaged in the aforementioned cross-border transfers, you are recommended to adopt the RMCs, and when adopting the RMCs, the New Guidance suggests that you may develop your own form of data transfer agreements or incorporate RMCs into a wider service agreement.

According to the New Guidance, as a matter of good practice and observance with the DPPs under the PDPO, in the event of any transfers of personal data outside Hong Kong, you should also notify data subjects of the transfer and the underlying grounds of such to ensure transparency between data users and data subjects. You are encouraged to make such notifications through adequate privacy policies and privacy notice. Where necessary, you may also implement internal compliance policies and measures with respect to the handling of cross-border data transfers for your personnel to ensure compliance.

Next steps:

The New Guidance provides Hong Kong data users with some useful guidance when implementing cross border transfers. Although compliance with the New Guidance is not mandatory, data users that adopt the RMCs are likely to be in a better position to demonstrate that they have considered the relevant risks relating to cross border data transfer, have implemented appropriate measures or practices to mitigate the impact of such risks in the event of any alleged breaches, and avoid any potential liability and reputational damage.

The New Guidance is potentially a sign that the implementation of Section 33 of the PDPO, or an updated and modified version of this section, may be imminent. Nevertheless, until Section 33 of the PDPO comes into force, the RMCs will likely only be adopted by those data users that are willing to adopt such provisions as a matter of international best practice.

Singapore

Latest developments:

Beginning 1 October 2022, enhanced financial penalties for a breach of data protection obligations under the PDPA have come into effect.

Summary:

Under the PDPA, the PDPC may impose a financial penalty if it determines that an organisation has intentionally or negligently contravened its data protection obligations.

Previously, the maximum financial penalty under the PDPA was SGD 1 million (approximately USD 700,000 or EUR 700,000).

On 1 October 2022, amendments to the PDPA took effect which increased the maximum financial penalty for a breach of data protection obligations to the higher of:

- 10% of an organisation's annual turnover in Singapore, where the annual turnover exceeds SGD 10 million (approximately USD 7 million or EUR 7 million);
- SGD 1 million (approximately USD 700,000 or EUR 700,000).

How could it be relevant for you?

Organisations, particularly those with annual turnover of more than SGD 10 million in Singapore, should note that they could be subject to the enhanced financial penalties of up to 10% of annual turnover, if they intentionally or negligently breach their data protection obligations under the PDPA.

Next steps:

The PDPC may in future impose a financial penalty above SGD 1 million (approximately USD 700,000 or EUR 700,000) in an appropriate case. It remains to be seen in what circumstances the PDPC will decide that it is warranted to do so.

Singapore

Latest developments:

The Singapore Court of Appeal held in *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 (***Bellingham***) that emotional distress suffered as a result of a contravention of the PDPA can constitute "loss or damage", for which an aggrieved individual may commence civil proceedings in court to seek relief. The Court of Appeal clarified that an individual's right of private action under the PDPA is not limited to the traditional heads of loss or damage recognised under common law (i.e., pecuniary loss, damage to property and personal injury).

Aggrieved individuals whose personal data is the subject of a breach of PDPA obligations may seek recourse by complaining to the PDPC, and/or by commencing a private action in respect of loss or damage suffered.

Summary:

Under Section 48O of the PDPA, an individual who suffers loss or damage directly as a result of an organisation's contravention of its data protection obligations may commence civil proceedings in court for relief. The court may grant the individual:

- Relief by way of injunction or declaration;
- Damages; or
- Any other relief as the court thinks fit.

In *Bellingham*, the plaintiff's personal data had been used by the defendant in breach of the PDPA for the purpose of marketing certain financial products to the plaintiff. The plaintiff did not suffer any pecuniary loss as a result, but claimed relief in court for loss or damage in the form of: (a) emotional distress; and (b) loss of control of his personal data.

The Court of Appeal held that emotional distress constitutes a form of actionable loss or damage within the meaning of the PDPA, on the basis that this interpretation is consistent with Parliament's intent. However, mere loss of control over personal data would not constitute such loss or damage, since a breach of PDPA obligations would inevitably involve a loss of control over an individual's personal data, which would render the phrase "loss or damage" tautologous.

The Court of Appeal therefore decided to grant relief in the form of: (a) an injunction restraining the defendant from using, disclosing or communicating the plaintiff's personal data; and (b) an order that the defendant undertake to destroy the plaintiff's personal data.

How could it be relevant for you?

Organisations may wish to consider whether their existing data protection policies and contractual arrangements adequately protect against the risk of civil liability under the PDPA, apart from enforcement action such as financial penalties taken by the PDPC.

Next steps:

The Court of Appeal's decision in *Bellingham* makes clear that, under Singapore law, a breach of PDPA obligations does not have to result in pecuniary loss before an individual can exercise the right of private action, and that emotional distress is actionable as a form of loss or damage. This is an alternative means for aggrieved individuals to seek recourse, aside from making a complaint to the PDPC.

In *Bellingham*, the relief granted was in the form of an injunction and order for destruction of personal data. It remains to be seen if the Singapore courts will in a future case award damages to an aggrieved individual who has not suffered any pecuniary loss, and how such damages would be quantified (if any).

Singapore

Latest developments:

In July 2022, the PDPC issued the Guide on Personal Data Protection Considerations for Blockchain Design (**Blockchain Guide**). The Blockchain Guide provides guidance to organisations on complying with the PDPA when deploying blockchain applications that process personal data, as well as on data protection by design (**DPbD**) considerations for more accountable management of personal data. While the Blockchain Guide focusses on blockchain technology, the principles and recommendations set out therein may also be broadly applicable to certain distributed ledger technologies.

Summary:

The Blockchain Guide is aimed at organisations that:

- Govern, configure and operate blockchain networks and consortia (blockchain operators);
- Design, deploy and maintain applications on blockchain networks (application service providers); and
- Use blockchain applications (participating organisations).

Key takeaways from the Blockchain Guide include the following:

- Personal data is stored on blockchains in a decentralised fashion, and data tends to be tamper-resistant as it cannot be directly edited or deleted. This leads to compliance issues relating to (i) accountability – as it may be challenging to assign data controllership over on-chain personal data, especially if node operators are unknown; and (ii) immutability – as it may be challenging to enable data correction or deletion.
- Personal data should not be stored on a permissionless blockchain whether in-clear, encrypted or anonymised, unless the individual has given consent to public disclosure of their personal data. This is because it is difficult in practice to protect and ensure accountability over personal data on permissionless blockchain networks, owing to the anonymity of public nodes and lack of access controls.

Singapore

- Personal data written on-chain on a permissioned blockchain should be encrypted or anonymised using industry standard algorithms or practices. Access should be provided only to authorised blockchain participants who require the data for business purposes, through the use of decryption keys or identity matching tables provided through off-chain channels. Data correction should be enabled through the insertion of new entries with encrypted corrected data, and the disposal of decryption keys of unneeded or erroneous data should be mandated to render such data indecipherable. Blockchain operators should implement and enforce legally binding consortium agreements or contracts, with clear data controller or data intermediary obligations.
- Application service providers should design their applications so that personal data is stored in an off-chain database or data repository where traditional access control mechanisms can be instituted. Only a hash of the personal data or a hash of the link to the off-chain database should be written on-chain.

How could it be relevant for you?

Organisations that utilise blockchain technologies in data processing activities should note the recommendations set out by the PDPC in the Blockchain Guide. While the Blockchain Guide is not legally binding *per se*, compliance with the PDPC's guidelines could be considered to be a relevant factor in any future assessment undertaken by the PDPC of whether an organisation has met its obligations under the PDPA.

Next steps:

The PDPC intends for the Blockchain Guide to be updated and revised regularly to remain relevant, given the fast-changing nature of the blockchain industry.

Singapore

Latest developments:

In previous amendments to the Personal Data Protection Act 2012 (**PDPA**) passed by the Singapore Parliament, new provisions were enacted to introduce a new data portability obligation. When the new provisions on data portability are brought into effect, they will enable individuals to give a data porting request to an organisation to transmit their personal data to another organisation under certain conditions.

Summary:

The new data portability obligation is intended to:

- Provide individuals with greater autonomy and control over their personal data; and
- Facilitate the innovative and more intensive use of applicable data in the possession or under the control of organisations to support the development, enhancement and refinement of goods and services.

Further implementing details of the data portability obligation are expected to be made available by the Personal Data Protection Commission (**PDPC**) and set out in regulations prior to the bringing into effect of the data portability obligation.

Where the data portability obligation applies, an organisation will be required to, at the request of an individual, transmit his or her personal data that is in the organisation's possession or under its control to another organisation in a commonly used machine-readable format. The data portability obligation will only apply to data in electronic form, and to organisations that have an ongoing relationship with the individual who makes the porting request. The data portability obligation will not apply to derived personal data, i.e., personal data derived by an organisation in the course of business from other personal data.

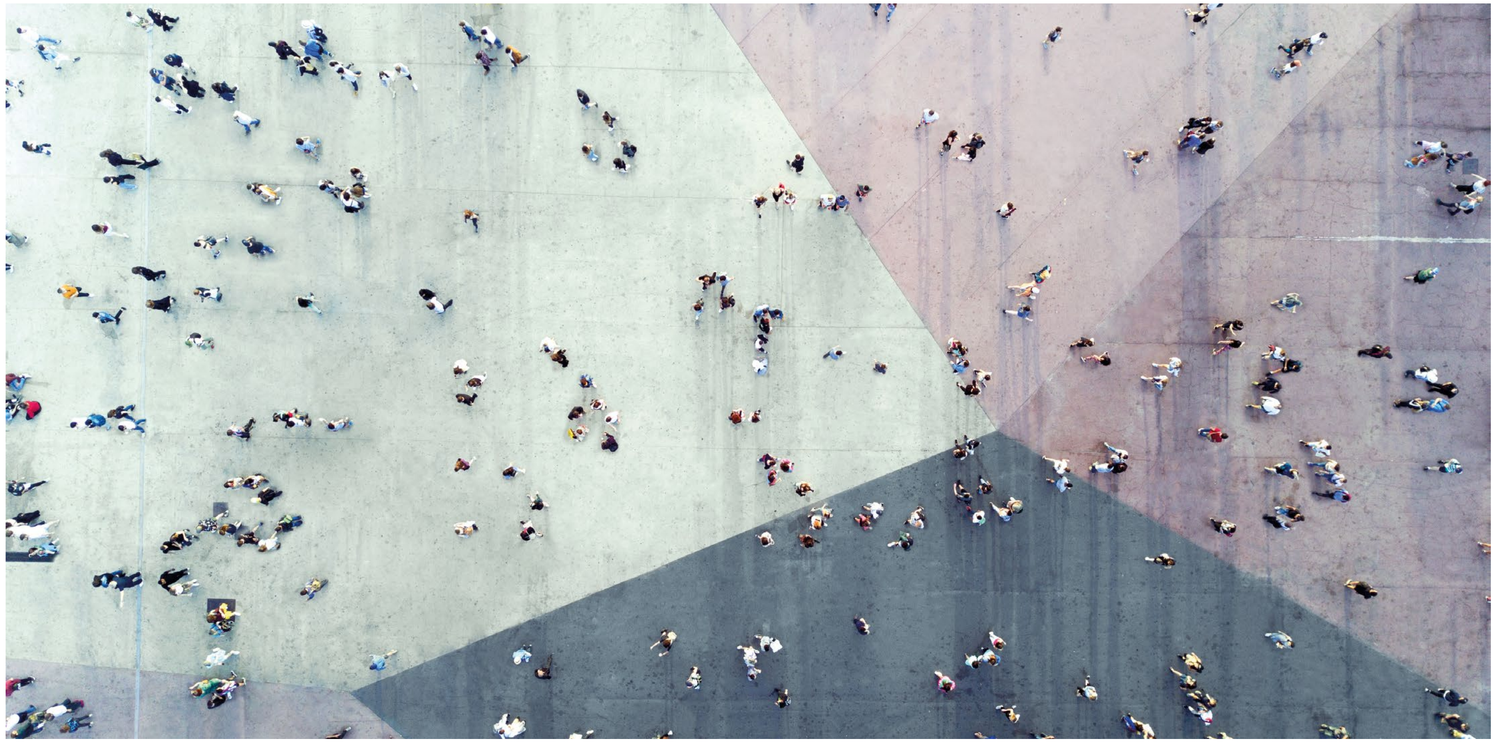
Singapore

How could it be relevant for you?

Organisations should monitor developments in this area to determine whether and the extent to which they may be subject to the data portability obligation, once the detailed scope of the obligation is made available. Organisations that are subject to the data portability obligation should consider taking steps to give effect to the obligation, such as by putting in place processes and training staff to operationalise the handling of data porting requests.

Next steps:

Implementing details of the data portability obligation are expected to be set out in regulations which will be issued subsequently. The regulations will likely provide clarity on the classes of organisations and personal data that will be subject to the data portability obligation. The legislative provisions establishing the data portability obligation are expected to be brought into force after the implementing regulations are ready and there is greater clarity on the scope of the data portability obligation.



Cyber-security

CHAPTER 5

Australia

Federal Cybersecurity Review (February 2023) - 1/2

Security of Critical Infrastructure Act 2018 (Cth) Reforms

Data Security

Latest developments:

In addition to the Privacy Act review mentioned in chapter 4, which includes recommendations regarding security of personal information, in February 2023, the Albanese Government released a discussion paper considering various options for reform in respect of cybersecurity (**Cybersecurity Review Report**).

Summary:

An Expert Advisory Board appointed by Australia's first ever Minister for Cyber Security, the Honourable Claire O'Neil MP, released a Cybersecurity Review Report regarding the development of Australia's Cyber Security Strategy for 2023-2030 (**Strategy**). The Strategy will be progressed in parallel with the Australian Government's other digital and data related priorities, including the Attorney General Department's review of the Privacy Act and the ACCC's Digital Platform Services Inquiry 2020-25.

Three core areas of policy which will be included in the Strategy are:

- Enhancing and harmonising regulatory frameworks;
- Strengthening Australia's international strategy on cyber security; and
- Securing government systems.

Proposals to facilitate the Strategy include:

- Whether obligations on company directors should specifically address cyber security risks and consequences;
- Whether Australia should introduce a Cyber Security Act (with an aim to draw together existing (and, likely, future) cyber-specific legislative obligations and standards across industry and government) and what should be included in any such legislation;
- Whether the definition of 'critical infrastructure asset' under the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) should be broadened to include customer data and systems (our articles about the SOCI Act can be found here and here);
- In relation to the payment of ransoms and extortion demands by cyber criminals:
  - Whether the Government should prohibit payment by victims of cybercrime and/or insurers and, if so, under what circumstances;
  - Whether the Government should clarify its position regarding the payment of ransoms by companies and the circumstances in which this may constitute a breach of law (for example, currently this may be caught by terrorism financing legislation or the sanctions regime); and

Australia

Federal Cybersecurity Review (February 2023) - 2/2

Security of Critical Infrastructure Act 2018 (Cth) Reforms

Data Security

  - Whether a mandatory reporting regime should be implemented in respect of such payments;

- Whether reporting and response requirements following a major cyber incident should be streamlined; and

- Whether an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) would improve engagement with organisations that experience a cyber incident in order to allow information to be shared between the organisation and ASD/ACSC without the concern that such information would be shared with regulators.

The Department is also seeking feedback on broader policy questions, including how:

- Australia could establish itself as the most cyber secure nation in the world by 2030;

- To monitor the regulatory burden on businesses so as to make cyber security obligations clear and easy to follow, both from an operational perspective and for company directors (given the existing framework includes a range of implicit and overlapping obligations on entities), particularly for small and medium-sized enterprises;

- To increase support available to victims of cybercrime; and

- To improve information sharing with industry in relation to cyber threats, for example by sharing root cause findings from investigations of major cyber incidents.

Next steps and relevance:

Industry, and the wider community, have until 15 April 2023 to provide feedback on what should be included in the Strategy. The Cybersecurity Review Report includes several specific proposals which, if realised, would have a significant impact on business operations and management. Security of Critical Infrastructure Act 2018 (Cth) Reforms

Australia

Federal Cybersecurity Review (February 2023)

Security of Critical Infrastructure Act 2018 (Cth) Reforms

Data Security

Latest developments:

In November 2021, the Australian Parliament passed the first phase of reforms to the SOCI Act. The legislation was given royal assent in December 2021. Subsequently, the Australian Parliament passed the second phase of reforms on 31 March 2022 and the legislation was given assent on 1 April 2022.

Summary:

The first phase of reforms expands the scope of the SOCI Act by:

- Introducing new 'critical infrastructure sectors', including the communications and data storage or processing sectors;
- Imposing obligations relating to mandatory cyber-incident reporting (including within 24 and 72 hour timeframes); and expanded requirements to provide information to the Register of Critical Infrastructure Assets. However, these obligations will not automatically apply and instead need to be 'switched on' by rules underlying the SOCI Act (subject to grace periods); and
- Granting the government a range of new powers, including to intervene, seek information and compel action in the event of a cybersecurity incident.

The second phase of the reforms introduces obligations to maintain risk management programs and additional cybersecurity obligations on critical infrastructure assets designated as systems of national significance. The requirements for risk management programs also need to be 'switched on'.

How could it be relevant for you?

The reforms are relevant to businesses responsible for or who own critical infrastructure assets. Such businesses will need to have reporting and other mechanisms in place to ensure compliance if the rules are applicable and any grace periods have lapsed.

Next steps:

A set of rules which 'switches on' certain obligations under Part 2 (Register of Critical Infrastructure Assets) and Part 2B (Notification of cyber security incidents) of the SOCI Act was finalised on 6 April 2022. The grace periods for reporting obligations ended on 8 October 2022.

A set of draft rules relating to Risk Management Programs has also been released, while the consultation period for these rules closed on 18 November 2022.

Australia

Federal Cybersecurity Review (February 2023)

Security of Critical Infrastructure Act 2018 (Cth) Reforms

Data Security - 1/2

Latest developments:

In April 2022, the Department of Home Affairs (under the Morrison Government) released a discussion paper seeking views on the development of Australia's National Data Security Action Plan (**Action Plan**). The Action Plan forms part of the government's 'Digital Economy Strategy' and aims to define a set of national, whole-of-economy expectations for data security for governments, businesses and individuals. Consultation on the Action Plan closed in June 2022.

Discussion Paper

'Data security' is defined in the Discussion Paper as a 'broad term that refers to protecting the information collected, processed and stored on digital systems and networks.' In contrast to privacy, which seeks to protect personal and sensitive information from unauthorised access, data security seeks to address unauthorised access to *all* data types.

In the Discussion Paper, the government notes that the current data security regulatory environment is 'complex and contested', with different initiatives targeting different parts of the economy. It notes that there is no common standard for the protection of similar data sets held by different jurisdictions Action Plan seeks to align and build on existing data security settings across the economy.

In developing the Action Plan, the government plans to consider:

- How to strengthen and coordinate data security across the broader economy;
- Measures to ensure that the data of all Australians is appropriately controlled and accountable;
- Ensuring all Australians know their rights, roles and responsibilities when it comes to the secure handling, storing and managing of data;
- Ensuring data security guidance, in both policy and legislation, is consistent across jurisdictions;
- Promoting alignment across data security requirements established under other data and digital initiatives, including the Consumer Data Right;
- Outlining Australia's international data security obligations and the risks posed to national security if data is obtained by foreign actors or cyber criminals; and
- Policy options to support whole of economy data security uplift and digitalisation to support the aim of becoming a leading digital economy by 2030.

Three pillars (security, accountability and control) will underpin the Action Plan. The Action Plan complements the recent reforms to the *Security of Critical Infrastructure Act* 2018.

Australia

Federal Cybersecurity Review (February 2023)

Security of Critical Infrastructure Act 2018 (Cth) Reforms

Data Security - 2/2

Next steps:

Public consultation on the Action Plan closed on 24 June 2022 and further developments are expected in 2023.

China

Cybersecurity review

Recent Regulatory Action:
DiDi Case

Latest developments:

China's cybersecurity review system was first introduced into law by the CSL, which requires CII operators to apply for national security review on their procurement of network product and services if it may impact national security. The cybersecurity review regime has been further updated and implemented by the *Measures for Cybersecurity Review* (**Review Measures**) which came into effect on February 15, 2022.

Summary:

The Review Measures extend the scope of cybersecurity review from procurement by CII operators to also include data processing activities by network platform operators that impact or may impact national security. Notably, a network platform operator must also apply for a cybersecurity review over its proposed listing outside China, if the network platform operator controls over one million users' PI.

The Review Measures provide that the cybersecurity review should take into account the following aspects

- The risks of illegal control of, interference in, or destruction of CII arising from the use of the products and services;
- The harm to the business continuity of CII caused by the interruption of the supply of the products and services;
- The security, openness, transparency, diversity of sources of products and services, reliability of supply channels, and the risks of supply disruption caused by political, diplomatic, and trade factors;
- The compliance by product and service providers with Chinese laws, administrative regulations, and departmental rules;
- The risks of core data, important data, or a large amount of personal information being stolen, leaked, damaged, illegally used, or illegally transferred to another jurisdiction;
- The risks of the CII, core data, important data or a large amount of personal information being affected, controlled or maliciously used by foreign governments and network information security risks after listing; and
- Other factors that may endanger the security of CII, cybersecurity, and data security.

The time limit for a cybersecurity review is 30 working days for review and 15 working days for reply under normal situations and can be extended by 15 working days. Notably, for cases where the relevant ministries cannot reach a consensus, the case will follow a special review procedure, and the statutory time limit can be extended for 90 working days or longer.

China

Cybersecurity review

Recent Regulatory Action: DiDi Case - 1/2

Latest developments:

On July 21, 2022, the CAC issued its penalty decision to Didi Global Inc. (**Didi**) after over 12 months' investigation since it launched a cybersecurity review over Didi and two other companies last July. The penalties include a fine of CNY 8.026 billion on Didi and a fine of CNY 1 million on each of the Chairman and CEO.

Summary:

According to the news release issued by the CAC, Didi had violated the CSL, the DSL and the PIPL. The CAC said that the facts of the violations are clear, the evidence is conclusive, the circumstances are serious and the nature is vile.

Didi was found to have committed 16 law violations covering eight aspects:

- The illegal collection of screenshot information from users' phone albums;
- The excessive collection of users' clipboard and App list information;
- The excessive collection of passengers' information about facial recognition, age, job, family relationships and hailing address;
- The excessive collection of precise location (latitude and longitude) information;
- The excessive collection of drivers' education information and the storage of drivers' unredacted ID number information;
- The analysis of passengers' travel intentions, city of residence and non-local business/travel information without clearly informing the passengers;
- Frequent requests of irrelevant "phone call permissions" when offering ride-hailing service; and
- Failure to accurately and clearly explain the purpose of processing 19 types of personal information such as users' device information.

In addition, the CAC said that a previous cybersecurity review also found that Didi had engaged in data processing activities that seriously affected national security and violated other laws and regulations such as refusing to comply with explicit requests from the regulators and intentionally evading supervision.

China

Cybersecurity review

Recent Regulatory Action: DiDi Case - 2/2

Next steps and relevance:

While the scope of CII, core data and important data is yet to be clarified, the recent enforcement action against Didi seems to indicate that the CAC might elect to enforce the Review Measures where necessary. As such, network platform operators should start to assess whether their processing activities impact or may impact national security and therefore trigger the cybersecurity review process.

Hong Kong

New cybersecurity legislation proposed- 1/2

New guidance on Data Security Measures for Information and Communications Technology issued

Latest developments:

The plan to introduce new legislation to strengthen the cybersecurity of critical information infrastructure in Hong Kong (the **"Plan)** was first announced in the 2021 Policy Address.

In April 2022, the Innovation and Technology Bureau and the Office of the Government Chief Information Officer submitted a paper on information security which, amongst others, provides updates of the Plan to the Panel on Information Technology and Broadcasting of the Legislative Council.

On 25 May 2022, in a written reply to Legislative Council regarding questions on cybersecurity standards in Hong Kong (the **"Written Reply)**, the Secretary for Innovation and Technology confirmed that preparatory work to clearly define cybersecurity obligations of critical information infrastructure operators (**CII operators)** in Hong Kong is underway.

Summary:

With a view to strengthening the cybersecurity of critical information infrastructures in Hong Kong, the Policy Addresses in two consecutive years of 2021 and 2022 both promoted the establishment of a management system by CII operators coupled with the Government's proposal for the enactment of cybersecurity legislation.

The key takeaways from the Written Reply are as follows:

- Legislation specific to cybersecurity of critical information infrastructures is needed to supplement the guidelines and requirements imposed by individual regulatory bodies in formulating a unified approach to cybersecurity in Hong Kong;
- The legislative proposals will reference cybersecurity standards adopted by other jurisdictions around the world; and

According to the Report of the Panel on Security for submission to the Legislative Council, dated 7 December 2022, the public consultation has been postponed to early 2023.

Details of the proposed legislation have yet to be revealed but the following would have a bearing on the effect and direction of the proposed legislation:

- The proposed scope of the regulation and terms such as "CII operators" and "network operators";
- Whether there would be any restrictions on the transfer of data collected or generated by CII operators out of Hong Kong; and
- The proposed authority for oversight and enforcement of the proposed legislation.

Hong Kong

New cybersecurity legislation proposed - 2/2

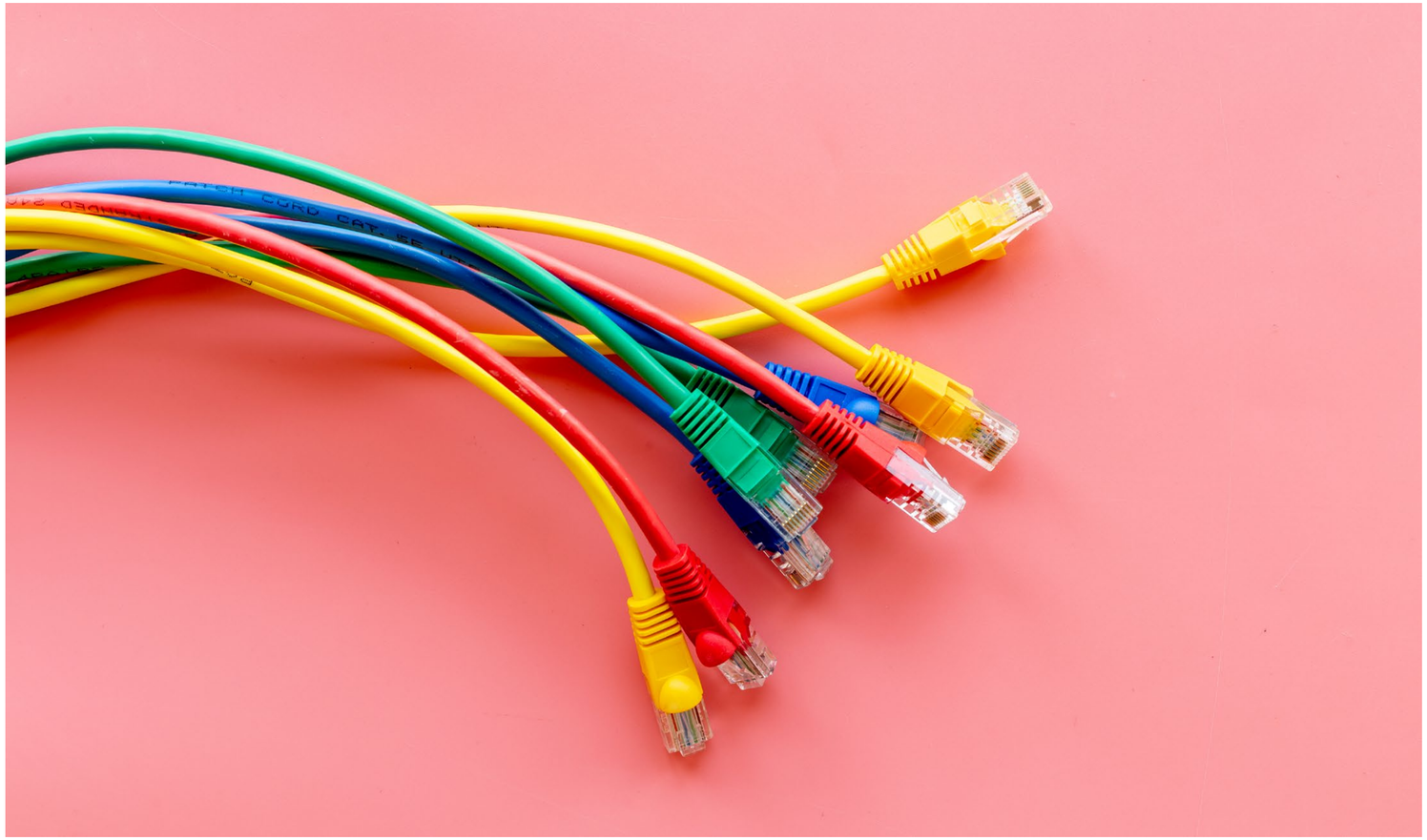
New guidance on Data Security Measures for Information and Communications Technology issued

How could it be relevant for you?

Interested parties, such as finance, telecommunications and technology companies dealing with critical information infrastructure, should observe the upcoming public consultation and details of the proposed legislative changes and assess the likely impact to their operations.

Next steps:

A public consultation exercise on the newly proposed cybersecurity legislation is expected to take place in early 2023. Given the developments in cyber security legislation globally and in particular in China in recent years, it is expected that similar legislation will be introduced in Hong Kong in the near future.



Hong Kong

New cybersecurity legislation proposed

New guidance on Data Security Measures for Information and Communications Technology issued - 1/3

Latest developments:

On 30 August 2022, the Privacy Commissioner of Personal Data (**PCPD)** issued the "Guidance Note on Data Security Measures for Information and Communications Technology" (the **"ICT Guidance)** to provide data users with recommended data security measures for ICT to facilitate compliance with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO)**.

Summary:

Pursuant to Data Protection Principle 4 of the PDPO, data users in Hong Kong should take all practical steps to ensure that any personal data held by the data user is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to a number of factors such as the kind of data held, the physical storage location, the security measures adopted in the storage medium, and the security measures taken in transmission and access. Data security is one of the key obligations of data users that is integral to a number of other data protection principles under the PDPO.

In the light of the increase in cybersecurity incidents, the ICT Guidance provides data users with recommended data security measures to prevent malicious attacks on their information systems and ensure compliance with the requirements under the PDPO.

The ICT Guidance provides recommendations on data security measures in the following seven (7) areas, supplemented by case studies:

- **Data Governance and Organisational Measures**
  Data users are recommended to establish clear internal policy and procedures on data governance and data security, covering the following areas:
  - Respective roles and responsibilities of staff in maintaining the information and communications systems and safeguarding data security;
  - Data security risk assessments;
  - Accessing data in and exporting data from the information and communications systems;
  - Outsourcing of data processing and data security work;
  - Handling data security incidents, including incident response plan and reporting mechanism; and
  - Destruction of data that is no longer necessary for the original purposes of collection or related purposes.

Hong Kong

New cybersecurity legislation proposed

New guidance on Data Security Measures for Information and Communications Technology issued - 2/3

While adoption of international best practices and standards (e.g. ISO/IEC 27000 family of Information Security Management Systems standards) may be used, the ICT Guidance emphasises that the adequacy of security measures will depend on the circumstances of each case, and a data user should review and revise its internal data security policies and procedures to keep up with new industry standards and address new threats to data security, as well appoint suitable personnel and conduct sufficient training to ensure ongoing compliance.

- **Risk Assessments on data security for new systems and applications**
  Consistent with the PCPD's approaches in relation to data protection compliance, data users are recommended to conduct risk assessments on data security for new systems and applications before launch, and periodically in accordance with data security policy and procedures. The risk assessments will consider factors including the sensitivity of the data being processed by the new systems and applications, as well as potential harm arising from leakage or unauthorised access to such data. The ultimate objective is to ensure that security risks are addressed before new systems and applications commence collection and processing of personal data.

- **Technical and Operational Security Measures**
  The ICT Guidance sets out a non-exhaustive list of technical and organisation measures that a data user may consider putting in place to ensure data security, including adopting:
  - Measures to secure computer networks;
  - Database management;
  - Access control measures;
  - Adoption of firewalls and anti-malware;
  - Protecting online applications;
  - Encryption measures in relation to data such as tokenisation and hashing;
  - Security measures relating to emails and file transfers;
  - Backup, destruction and anonymisation

- **Data Processor Management**
  Data processors that solely process personal data on behalf of data users but do not process personal data for their own purposes are not directly regulated under the PDPO. Accordingly, the ICT Guidance provides some practical guidance on how data users may seek to adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of data transferred to data processors for processing.

Hong Kong

New cybersecurity legislation proposed

New guidance on Data Security Measures for Information and Communications Technology issued - 3/3

- **Remedial actions in the event of Data Security Incidents**
  Although the PDPO does not currently contain mandatory data breach reporting obligations, data users are recommended to take timely and effective remedial actions after the occurrence of a data security incident to reduce the risks of unauthorised or accidental access, processing or use of personal data. The ICT Guidance sets out some common remedial actions including changing system configurations, changing passwords, ceasing access rights of users, notifying affected individuals, notifying PCPD etc. In essence, it is recommended that data users follow the PCPD's Guidance on Data Breach Handling and Giving of Breach Notifications*.

- **Monitoring, evaluating and improving compliance with data security policies**
  The ICT Guidance suggests that a data user may commission an independent task force, such as an internal or external audit team, to periodically monitor compliance with the data security policy and evaluate the effectiveness of its data security measures.

- **Other recommended data security measures for cloud services, "Bring Your Own Devices" and portable storage devices**
  With the wide adoption of cloud technologies, BYOD and use of portable storage devices, the ICT Guidance also provides some specific recommendations on the adoption of data security measures in such scenarios, for example, setting up strong access control and authentication procedures for a cloud-based environment and reviewing cloud-based security features available to apply the appropriate features.

How could it be relevant for you?

Although compliance with the ICT Guidance is not mandatory, data users in Hong Kong are advised to refer to the ICT Guidance for practical guidance, as well as to work with data security experts and legal advisers to ensure relevant data security requirements under the PDPO are met. Further, in face of the rapid developments in the digital economy, IT consultants and advisers are suggested to refer to the ICT Guidance for insights and recommendations on how to assist data users in Hong Kong to comply with the data security obligations under the PDPO.

Next steps:

The data security measures set out in the ICT Guidance are for general reference to assist data users to ensure data security in the data processing and data management life cycle. They give practical insights to data users on the technical and organizational measures that the PCPD considers appropriate and relevant.

* https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

Singapore

Licensing Framework for Cybersecurity Service Providers - 1/2

Latest developments:

On 11 April 2022, a new licensing framework for cybersecurity service providers (**CSPs**) under Part 5 of the Cybersecurity Act 2018 (**CA**) came into effect. CSPs that provide licensable cybersecurity services to the Singapore market must obtain a licence from the Cybersecurity Services Regulation Office (**CSRO**).

The new licensing framework is intended to be a light-touch regime. It aims to: (a) improve security and safety; (b) raise the quality and improve the standing of CSPs; and (c) address information asymmetry.

Summary:

The CA specifies two licensable cybersecurity services:

- Managed security operations centre (**MSOC**) monitoring services; and
- Penetration testing services.

A MSOC monitoring service is defined as a service for the monitoring of the level of cybersecurity of a computer or computer system of another person by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system.

A penetration testing service is defined as a service for assessing, testing or evaluating the level of cybersecurity of a computer or computer system, by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system, and includes any of the following activities:

- Determining the cybersecurity vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of;
- Determining or testing the organisation's ability to identify and respond to cybersecurity incidents through simulation of attempts to penetrate the cybersecurity defences of the computer or computer system;
- Identifying and quantifying the cybersecurity vulnerabilities of a computer or computer system, indicating vulnerabilities and providing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk;
- Utilising social engineering to assess the level of vulnerability of an organisation to cybersecurity threats.

Singapore

Licensing Framework for Cybersecurity Service Providers - 2/2

Service providers that provide licensable cybersecurity services to the Singapore market must obtain a licence(s) from the CSRO. Service providers that offer both services will need to obtain a separate licence for each service.

The licensing requirements apply to CSPs regardless of whether they are companies or individuals (i.e., freelancers or sole proprietorships), and whether they are directly engaged to provide such services to customers or act as third-party CSPs providing services in support of other CSPs. The licensing requirements also apply to resellers and overseas CSPs who provide licensable cybersecurity services to the Singapore market.

Key regulatory obligations include ensuring that the licensed entity and its officers satisfy "fit and proper" criteria, keeping records, notifying the CSRO of certain changes in information, and adhering to professional conduct standards.

Each licence is valid for a period of 2 years. The licence fees for business entities and individuals are SGD 1,000 (approximately USD 700 or EUR 700) and SGD 500 (approximately USD 350 or EUR 350) respectively. However, a 50% waiver of the licence fees will be granted for all licence applications that are lodged up to 10 April 2023 (inclusive) to support businesses due to the impact of COVID-19.

It is an offence under the CA to engage in the business of providing a licensable cybersecurity services without a valid licence. Furthermore, any person who provides a licensable cybersecurity service without a valid licence is prevented from bringing proceedings in court to recover any commission, fee, gain or reward for the service.

How could it be relevant for you?

Providers of MSOC monitoring services or penetration testing services to the Singapore market, regardless of where they are located in the distribution chain, may trigger licensing requirements and should assess the need to apply for a CSP licence if they carry on such activities.

Next steps:

The CSRO will continue to monitor industry trends to assess if any new types of cybersecurity services should be included in the licensing framework.

Presently, there are no quality requirements imposed on CSPs under the licensing framework. However, the CSRO will continue to watch developments in this space in considering whether any quality requirements should be introduced in future.

Digital Identity and Trust Services

CHAPTER 6

Australia

Trusted Digital Identity Bill Exposure Draft

NSW Digital ID

Australia

Trusted Digital Identity Bill Exposure Draft

NSW Digital ID

Latest developments:

In October 2021, the Morrison Government released an exposure draft of the Trusted Digital Identity Bill 2021 (**TDI Bill**). Central to the TDI Bill is the notion that the digital economy is not possible unless Australians have digital identities that are safe, secure and convenient, to prove their identity online.

Summary:

The purpose of the TDI Bill is to:

- Expand the Australian Government Digital Identity System (**AGDIS**) by enabling greater participation of state and territory governments and private sector entities;
- Enshrine various privacy and consumer protections in law, so that Australians can have confidence in the AGDIS and know that their personal information is safe and secure; and
- Establish a permanent, independent, transparent and accountable Oversight Authority with responsibility for governing the AGDIS and the TDIF accreditation scheme under the legislation.

If the TDI Bill is passed as currently drafted, once an entity achieves accreditation, the privacy and consumer protections it must adhere to a number of privacy and data requirements and restrictions.

How could it be relevant for you?

Entities looking to be accredited entities or relying entities should be aware of the benefits of signing up for such a program (noting that participation is voluntary) as well as the additional privacy and data security obligations that apply if you choose to do so.

Next steps:

The exposure draft of the TDI Bill underwent a consultation process in October 2021. It has not progressed since and is uncertain at this stage whether that the TDI Bill will be introduced by the Albanese Government to Parliament later in 2023.

Australia

Trusted Digital Identity Bill Exposure Draft

NSW Digital ID

Latest developments:

The NSW Government commenced its ‘NSW Digital ID’ project which will allow customers in NSW to prove their identity without using physical identity documents.

The project differs from the Federal Government’s already existing ‘myGovID’ by allowing users to prove their identity with not only government organisations, but also with businesses without having to disclose additional personal information (such as a driver’s licence).

Next steps:

The project is expected to go live in 2023 for use by customers in NSW. The NSW Government is also currently working with the Federal Government to enable the use of NSW Digital ID outside of NSW, by adopting a national Digital Identity ecosystem.

Consumer

CHAPTER 7

Australia

Singapore

Anti-Scam Ratings
for E-Commerce
Marketplaces

Australia

Proposed reform to the Competition and Consumer Act 2010 (Cth) - 1/2

Treasury Laws Amendment (More Competition, Better Prices) Act 2022

Recent regulatory action

Latest developments:

On 14 December 2021, Treasury released a Regulation Impact Statement (**RIS**) for consultation, which included recommendations for reforming the Australian Consumer Law (**ACL**), including introducing a civil prohibition for failing to provide a consumer guarantee remedy. The recommendations in the RIS were foreshadowed in the Cybersecurity Review Report (referred to in chapter 5) as providing consumers with more options to directly enforce consumer guarantees respect of cybersecurity incidents and digital goods.

Summary:

One of the findings in the Cybersecurity Review Report (referred to in chapter 5) is that there are limited legal options for consumers to seek remedies or compensation for cyber security incidents. The Home Affairs Department notes that:

- While companies cannot make misleading or deceptive representations about the cybersecurity of their products, there is no positive disclosure obligations in respect of cybersecurity under the ACL; and
- While the consumer guarantees may extend to digital goods, such application is untested.

Introducing a civil prohibition on failing to provide a consumer guarantee remedy is, in the view of the Home Affairs Department, desirable as it would provide the ACCC with more options to directly enforce the consumer guarantees under the ACL and address barriers associated with applying the guarantees in a cybersecurity context, for example:

- Consumers' lack of technical expertise to determine whether a breach of the consumer guarantees occurred because a good was not 'fit for purpose' or a service was not provided with 'all due care and skill'; and
- Determining whether a relevant transaction involves a 'good' or 'service' (as required under the ACL). As digital goods and services may consist of multiple components such as hardware, software and technology services, the Home Affairs Department notes that interpretations of current ACL provisions in previous cases (such as *Valve Corporation v ACCC* [2017] FCAFC 224) suggest that these components may not all fall within the scope of the ACL.

Australia

Proposed reform to the Competition and Consumer Act 2010 (Cth) - 2/2

Treasury Laws Amendment (More Competition, Better Prices) Act 2022

Recent regulatory action

How could it be relevant for you?

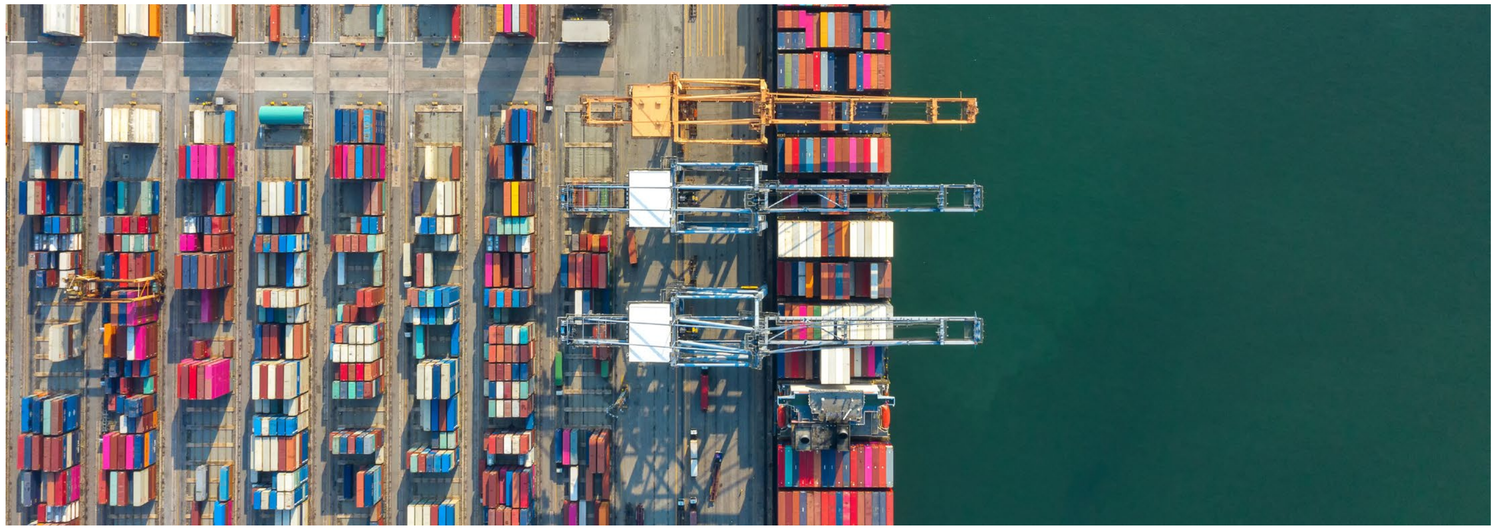
Businesses offering goods and services to consumers should be aware of the consumer guarantees set out in the ACL and how they might apply to digital goods and services or any cybersecurity incidents which occur. Such businesses should also be aware that enforcement action may result in response to non-compliance with the guarantees if the reforms suggested by the RIS are enacted into law.

Businesses should be aware of the increased risk of breaching the ACL or in using unfair contract terms. Businesses with standard form consumer or small business contracts should assess their current contract terms to determine if they are at risk of breaching the UCT regime before the amendment comes into effect in November 2023.

Next steps:

Consultation on the RIS was completed on 11 February 2022 and Treasury is currently in the process of reviewing submissions to determine the preferred policy/law reform approach to adopt. It is unclear at this stage whether the Albanese Government will pursue these reforms.

The *Treasury Laws Amendment (More Competition, Better Prices) Act* 2022 will come into effect on 9 November 2023, giving affected businesses a grace period of 12 months to amend their practices to become compliant.



Australia

Proposed reform to the Competition and Consumer Act 2010 (Cth)

Treasury Laws Amendment (More Competition, Better Prices) Act 2022

Recent regulatory action

Latest developments:

On 27 October 2022 the new Albanese Government passed the *Treasury Laws Amendment (More Competition, Better Prices) Bill* 2022, which received Royal Assent on 9 November 2022. This amendment increased penalties for engaging in anti-competitive conduct (for example, cartels, misuse of market power, and exclusive dealing) under Part IV of the *Competition and Consumer Act* 2010 and the *Australian Consumer Law*, and amends the unfair contract terms (**UCT**) regime contained within the ACL to afford more protections to consumers and small businesses.

Summary:

The *Treasury Laws Amendment (More Competition, Better Prices) Act* 2022 has two key functions as it relates to consumer protections in Australia. Firstly, the amendment increases the pecuniary penalty framework that businesses captured by the ACL are subject to when they breach the act.

Parties which breach the Act are now subject to maximum penalties of:

- For companies:
  - $50 million;
  - 3x the value of the benefit obtained, if that can be determined; or
  - If the value of the benefit cannot be determined, 30% of adjusted turnover during the breach turnover period (i.e. over the period the breach occurred, with a minimum of 12 months).
- For individuals:
  - $2,500,000

The amendment also substantively amends the unfair contract term (**UCT**) regime in the ACL to extend protections for consumers and small businesses.

Once the amendment comes into effect, the consequence of using or relying on unfair contract terms will significantly change. Currently, if a term was found to be unfair, the term would be void. However, from November 2023, including or relying on an unfair term is prohibited, and parties found to be using such terms may be subject to the newly-increased penalty framework set out above.

The amended UCT regime also expands the scope of contracts which are bound by it as a 'small business contract' will now include contracts where at least one party to the contract either employs less than 100 people (up from 20 people) or has an annual turnover of less than $10 million. As a result, more businesses will be protected by the UCT regime.

Australia

Proposed reform to the Competition and Consumer Act 2010 (Cth)

Treasury Laws Amendment (More Competition, Better Prices) Act 2022

Recent regulatory action - 1/2

Latest developments:

Despite there being no cases involving the application of consumer guarantees to data protection and privacy, the role of the ACCC is otherwise growing in relation to its regulation, as seen by enforcement action brought by the ACCC against various large digital platforms.

Summary:

In 2020, in proceedings initiated by the ACCC, the Federal Court found that HealthEngine engaged in misleading and deceptive conduct in respect of the sharing of patient information, ordering the payment of AU$2.9mil in penalties. The Court made this finding on the basis that HealthEngine had failed to adequately inform consumers that it provided their personal information to third-party insurance brokers.

The ACCC has targeted other large digital platforms, having brought separate proceedings against Google and Facebook in respect of their data practices, relying on, for example, the following sections of the ACL:

- 18, which prohibits misleading or deceptive conduct;
- 29(g)(1), regulating false or misleading representations; and
- 33, relating to conduct liable to mislead the public regarding the nature of goods.

More recently, the ACCC has commenced proceedings against Meta Platforms, Inc and Meta Platforms Ireland Limited (**Meta**) in relation to the publication of scam ads on Facebook. The scam ads allegedly encouraged investment in cryptocurrency or other 'money-making' schemes and displayed well-known Australian figures without their approval or endorsement.

The ACCC claims that the alleged conduct is in breach of Australian Consumer Law or the *Australian Securities and Investments Commission Act* 2001 (Cth).

The ACCC alleges false, misleading or deceptive conduct, and it claims that Meta 'aided or abetted or was knowingly concerned in false or misleading conduct and representations by the advertisers'. The ACCC claims that Meta was familiar with the ads and did not do enough to tackle the issue.

Australia

Proposed reform to the Competition and Consumer Act 2010 (Cth)

Treasury Laws Amendment (More Competition, Better Prices) Act 2022

Recent regulatory action - 2/2

How could it be relevant for you?

Businesses should be aware of the increasing role consumer law is playing in regulating data and privacy. Businesses that have, for example, misled consumers as to the collection of data, can face significant penalties under the ACL. In addition to ensuring compliance with privacy regimes, businesses should exercise care in relation to privacy notices and information given to consumers to ensure it doesn't breach the ACL.

Next steps:

The ACCC has now released its strategic priorities for 2022-2023, which include competition and consumer issues connected with digital platforms, as well as consumer and fair trading issues around 'manipulative or deceptive advertising and marketing practices in the digital economy'. The financial services sector, and in particular payment services, is also highlighted as a priority.

Singapore

Anti-Scam Ratings for E-Commerce Marketplaces - 1/2

Latest developments:

In May 2022, the Inter-Ministry Committee on Scams (**IMSC**) launched the E-commerce Marketplace Transaction Safety Ratings (**TSR**). TSR aims to provide consumers with information on anti-scam measures that major e-commerce marketplaces have in place.

The IMSC also launched the Revised Technical Reference 76 on Guidelines for Electronic Commerce Transactions (**TR 76**). The TR 76 aims to provide e-retailers and online intermediaries such as e-commerce marketplaces, with additional guidelines to better secure e-commerce transactions from scams. Together, TSR and TR 76 aim to raise consumer and industry awareness, and encourage the use of safety features and good practices when transacting online.

Summary:

TSR informs consumers of the transaction safety of different e-commerce marketplaces, based on the range of anti-scam measures they have in place. TSR covers major e-commerce marketplaces that facilitate online transactions from multiple sellers to multiple buyers, with a significant local reach or a significant number of e-commerce scams reported. E-commerce marketplaces are rated based on the extent to which they have implemented anti-scam measures that ensure (a) user authenticity, (b) transaction safety, (c) availability of loss remediation channels for consumers, as well as (d) the effectiveness of their anti-scam measures. The ratings range from one (lowest) to four (highest) ticks. To be awarded the full four-ticks, an e-commerce marketplace will need to implement all the critical anti-scam measures prescribed. Ratings are reviewed annually.

TR 76 is the national standard for e-commerce transactions. It has been revised to include additional best-anti-scam guidelines for e-retailers and e-commerce marketplaces. The additional anti-scam guidelines set out best practices for e-retailers and e-commerce marketplaces, relating to different areas of transactions, covering pre-, during- and post-purchase activities, customer support and merchant verification. The intent is to better enable merchant authenticity, improve transaction security and aid enforcement against e-commerce scams. As the TR76 guidelines form part of the safety features rated under TSR, e-commerce marketplaces that adopt the TR76 guidelines are more likely to score better on the TSR.

Singapore

Anti-Scam Ratings for E-Commerce Marketplaces - 2/2

How could it be relevant for you?

E-retailers and e-commerce marketplaces may wish to consider implementing the best-practice guidance set out under the TR76. E-commerce marketplaces with significant operations in Singapore should also note the possibility of being included in the list of marketplaces rated under TSR based on the level of their anti-scam measures in place.

Next steps:

The Singapore government will monitor this area to determine if further measures are required. It is expected that TSR ratings will be refreshed annually, while consumer advisories will be updated every six months.

Contacts

Australia

Shane Barber
Partner
+61 2 9226 9888
shane.barber@twobirds.com

Julie Cheeseman
Partner
+61 2 9226 9888
julie.cheeseman@twobirds.com

Michael Stojanovic
Special Counsel
+61 2 9226 9888
michael.stojanovic@twobirds.com

Rich Hawkins
Partner
+61 2 9226 9888
rich.hawkins@twobirds.com

Sophie Dawson
Partner
+61 2 9226 9888
sophie.dawson@twobirds.com

Hamish Fraser
Partner
+61 2 9226 9888
hamish.fraser@twobirds.com

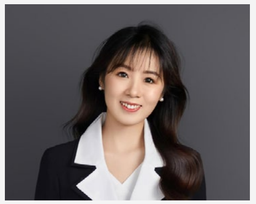
Thomas Jones
Partner
+61 2 9226 9888
thomas.jones@twobirds.com

Jane Owen
Partner
+61 2 9226 9888
jane.owen@twobirds.com

Contacts

China

James Gong
Partner
+86 10 5933 5688
james.gong@twobirds.com



Jacqueline Che
Associate
+86 10 5933 5688
jacqueline.che@twobirds.com

Hong Kong

Wilfred Ng
Partner
+852 2248 6000
wilfred.ng@twobirds.com

Gigi Cheah
Senior Consultant
+852 2248 6000
gigi.cheah@twobirds.com

"Bird & Bird is widely regarded as a longstanding leader in the TMT space."

Chambers Global 2023 – Ranked band 1 for TMT

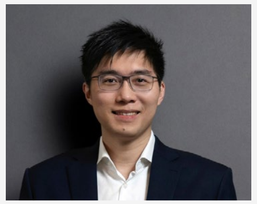
Contacts

Singapore

Jeremy Tan
Partner
+65 6534 5266
jeremy.tan@twobirds.com

Lijun Chui
Partner
+65 6534 5266
lijun.chui@twobirds.com

Loren Leung
Counsel
+65 6534 5266
loren.leung@twobirds.com

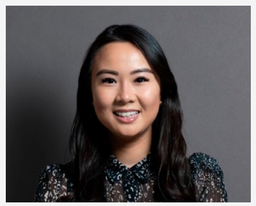


Shawn Ting
Counsel
+65 6534 5266
shawn.ting@twobirds.com

Elaina Foo
Associate
+65 6534 5266
elaina.foo@twobirds.com

Chester Lim
Associate
+65 6534 5266
chester.lim@twobirds.com

John Kuah
Associate
+65 6534 5266
john.kuah@twobirds.com



Florence Seow
Associate
+65 6534 5266
florence.seow@twobirds.com