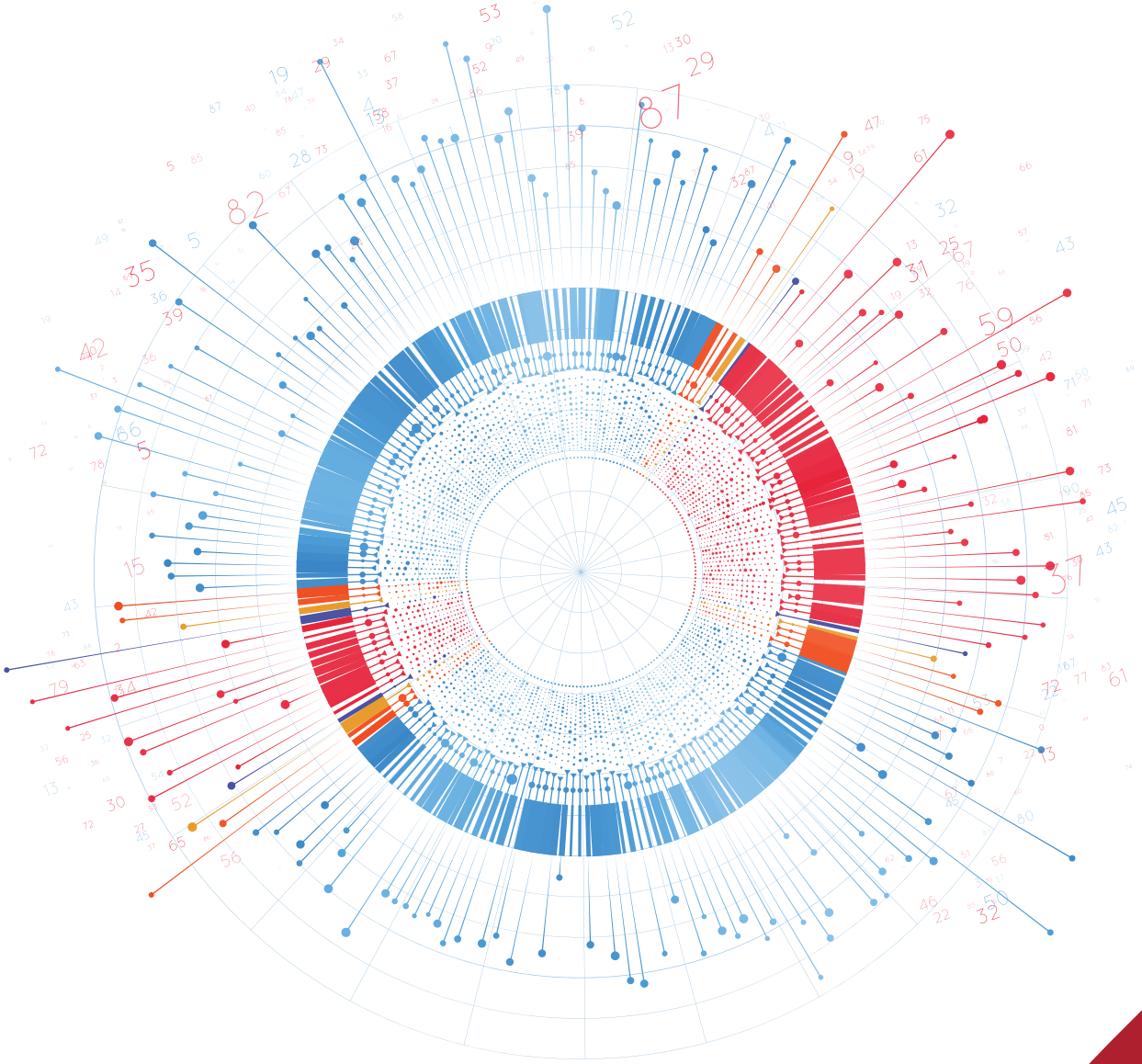
FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

2022

December

FSDC Paper No. 56



Connecting Data:
Establishing Hong Kong as a Cross-Boundary Financial Data Hub

Contents

- Executive Summary 1
- Background: Opportunities and Risks 2
  - Data as a strategic asset for financial services industry 2
  - Cross-boundary data flow to support the integration and digital transformation of the GBA 5
  - Hong Kong should position itself to be the financial data hub for the GBA 6
- Global data landscape and policies 8
  - Common mechanisms for cross-border/boundary data flows 8
  - The United States 10
  - The EU 11
  - Mainland China 12
  - Hong Kong 16
- Pain points facing Hong Kong's financial services industry 18
  - Lack of specific legislation to facilitate cross-border/boundary data transfers 18
  - The changing regulatory landscape of data protection 19
  - Operational obstacles 20
  - Compliance cost and challenges 21
  - Talent shortage 22
- Policy recommendations 23
  - To provide clarity on section 33 of PDPO 23
  - To strengthen data governance and policy coordination within the GBA 24
  - To formulate standard contractual clauses for cross-boundary data transfers within the GBA 30
  - To set up a third-party certification agency to conduct impartial conformity assessment on cross-boundary data transfers within the GBA 31
  - To explore the use of new technologies to enable cross-boundary data transfers within the GBA 32
  - To attract and cultivate talents with technological and digital-related skillsets 35
- Conclusion 38
- Appendices 39
  - Appendix 1. Key data regulation developments in Mainland China over the last five years 39
  - Appendix 2. A summary of data landscape and policies in Mainland China and Hong Kong 42
  - Appendix 3. AI ethical standards and requirements in Mainland China and Hong Kong and other international standards 43

Executive Summary

The financial services industry has become increasingly digitalised, with cross-border transactions continuing to grow significantly and data connectivity being an imminent business need globally. Similarly, within the Greater Bay Area (GBA), cross-boundary flow of data is crucial for the further integration and connectivity of the financial services industry. A coordinated governance framework and standard is key to facilitate data flow between Hong Kong and the rest of the GBA cities, and to address operational challenges and compliance uncertainties to businesses operating across multiple jurisdictions. Hong Kong, being the international financial centre (IFC) of Asia and already possessing robust information and communications technology infrastructure and innovation capabilities, has what it takes to become the financial data hub of the GBA to facilitate a frictionless flow of data within the region.

To this end, the Financial Services Development Council (FSDC) formed a Working Group consisting of industry experts to conduct a study with the aim of identifying challenges facing Hong Kong's financial services industry in data governance and putting forward recommendations to address them. We believe these recommendations will help establish Hong Kong as the financial data hub of the GBA, and thereby strengthen Hong Kong's status as an international financial centre. Our recommendations include:

- To provide clarity on section 33 of the Personal Data (Privacy) Ordinance
- To strengthen data governance and policy coordination within the GBA by the following means:
    - To establish white- and grey-lists to facilitate cross-boundary data transfers within the GBA
    - To explore the feasibility of cross-boundary data sharing through conducting pilot projects
    - To develop a set of GBA data governance standards
- To formulate standard contractual clauses for cross-boundary data transfers within the GBA
- To set up a third-party certification agency to conduct impartial conformity assessments on cross-boundary data transfers within the GBA
- To explore the use of new technologies to enable cross-boundary data transfers within the GBA
- To attract and cultivate talent with technological and digital-related skillsets

The FSDC recognised that data flow is a complex matter that requires thorough considerations concerning security, economic stability, and operating environment, among others. At the same time, the further integration of the GBA required a freer flow of data beyond the financial services industry. A better exchange of a broader range of data within the GBA (and beyond) will further enhance the integration of the GBA and support the growth of other sectors. While this paper has casted a focus on the freer flow of financial data within the GBA, the scope of the recommendations put forth here can be potentially expanded to cover other types of data and industries at a time that is considered appropriate by stakeholders concerned in the Mainland and Hong Kong. We believe these recommendations are some of the initial essential actions in helping establish Hong Kong as the financial data hub of the GBA, but also some of the first steps to further strengthen data connectivity within the region, thereby further deepening the integration of the GBA.

Background: Opportunities and Risks

The adoption of technology in financial services has rendered data as a strategic asset and, in return, data availability and quality can lend further support to the enhancement of the financial services industry. Such a trend is particularly important for cross-boundary businesses, which have benefited significantly through enhanced client experience and market connectivity.

Hong Kong – being Asia's leading international financial centre, a unique intermediary between Chinese and international markets, and home to many fintech companies – should take proactive actions to capture opportunities arising therein. It is believed that the city, which has an advanced IT infrastructure, communication network, and trusted legal system, is well positioned to become the financial data hub for the GBA to facilitate easier flow through the access, usage, and exchange of data within the region.

Data as a strategic asset for the financial services industry

According to the World Bank, "the digital economy is equivalent to 15.5% of global GDP, growing two and a half times faster than global GDP over the past 15 years" since 2007.[1] The global transformation to a digital economy has led major economies, including Mainland China, the European Union (EU), and the United States, among others, to attach strategic importance to data.[2] Data is now widely recognised as a key production factor, in addition to classical economic factors of production such as land, labour, and capital. Data is particularly important for the development of a digital economy.

Despite the importance of data, there is no consensus on the definition of data among the academic world and policy makers of different jurisdictions, as data can have multiple meanings depending on the context and jurisdiction. The matter is further complicated when it comes to defining a specific type of data, such as "personal data", as its scope usually varies significantly among legal jurisdictions. A review of studies shows that attempts to define data usually make a distinction between data and information – with information being commonly defined as refined and processed data,[3] and data generally being defined as a collection of unprocessed points about events, objects, and people.[4] These points can either be related or unrelated initially, but with aggregation, processing, and analysing, these points will become useful information for making decisions that have an impact on the economy, environment, health, or society in general.[5]

[1] World Bank, Digital Development, https://www.worldbank.org/en/topic/digitaldevelopment/overview (accessed on 16 June 2022)
[2] South China Morning Post (SCMP), US-China tech war: Beijing unveils grand plan to grow digital economy as US moves forward with competition bill (13 January 2022), https://www.scmp.com/tech/tech-war/article/3163246/us-China-tech-war-beijing-unveils-grand-plan-grow-digital-economy-us (accessed on 5 June 2022)
[3] United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)
[4] Organisation for Economic Co-operation and Development (OECD), Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies, https://www.oecd-ilibrary.org/sites/276aaca8-en/1/2/1/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book (accessed on 5 March 2022)
[5] United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)

Given the indispensable role of data, the usage and flow of data within a country and across borders have increased dramatically over the past few years. According to a study conducted by the United Nations in 2021 about digital economy, global internet traffic in 2022 was predicted to exceed all the internet traffic up to 2016.[6] It was estimated that 79 zettabytes (ZB, 1ZB = 1 trillion gigabytes) of data were created in 2021 alone,[7] and this number is expected to reach 180 ZB by 2025.[8] Notably, Mainland China is one of the biggest data generators, and is forecasted to generate 48.6ZB of data by 2025.[9]

The large and increasing amount of data is partly driven by the adoption of data-driven technologies in various industries to accelerate growth, capture new opportunities, expand access to other markets, and solve complex issues. Notably, innovative solutions are not only important at the time when an economy is doing well, but also crucial – and perhaps even more so – during times of crisis, natural disasters, and pandemics.Under these circumstances, digital savvy businesses are observed to fare better and can remain connected to their clients and customers, and hence remain competitive, and with better capability to weather through these challenging times.[10] As such, data can be seen as the lifeblood of businesses.

For the financial services industry in particular, its reliance on data is as much, if not more, than other industries. Financial services are data-driven with a significant amount of data involved. Activities within the financial services industry include processes to create, collect, store, transfer, and process data. The application of data in the financial services industry is omnipresent, including to support product development, improve sales and marketing efforts, better manage customer relationships, enhance risk management, strengthen internal management, and reinforce compliance monitoring.[11]

Take the banking industry of Hong Kong as an example; in 2020, the Hong Kong Monetary Authority (HKMA) established a financial data infrastructure, known as the Commercial Data Interchange (CDI), to facilitate the sharing of commercial data.[12] CDI is a consent-based financial infrastructure that would enable more secure and efficient data flow between banks and sources of commercial data. One benefit of CDI is its use as an alternative tool to facilitate banks in conducting risk assessment of loan applications from small and medium enterprises (SMEs). According to a study conducted by the HKMA in 2021, with the aid of CDI, 550 SME loans totalling over HKD 900 million were approved by the participating banks as of 1 November 2021.[13] With more efficient data sharing of the banking industry, SMEs have easier access to financing, therefore furthering financial inclusion.

---

[6] United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)

[7] Statista, Big data - Statistics & Facts, https://www.statista.com/topics/1464/big-data/#dossierKeyfigures

[8] https://www.red-gate.com/blog/database-development/whats-the-real-story-behind-the-explosive-growth-of-data (accessed on 5 June 2022)

[9] CNBC, As information increasingly drives economies, China is set to overtake the US in race for data (13 February 2019), https://www.cnbc.com/2019/02/14/china-will-create-more-data-than-the-us-by-2025-idc-report.html#:~:text=Data%20created%20and%20replicated%20in,to%2048.6ZB%20in%202025 (accessed on 2 June 2022)

[10] World Bank, Digital Development, https://www.worldbank.org/en/topic/digitaldevelopment/overview (accessed on 16 June 2022)

[11] Oxford University, Analytics: The real-world use of big data in financial services, https://www.ibm.com/downloads/cas/E4BWZ1PY (accessed on 16 June 2022)

[12] HKMA, Commercial Data Interchange, https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/commercial-data-interchange/ (accessed on 5 August 2022)

[13] HKSAR, Briefing to the Legislative Council Panel on Financial Affair (3 May 2022), Government, https://www.legco.gov.hk/yr2022/english/panels/fa/papers/fa20220503cb1-217-2-e.pdf (accessed on 5 August 2022)

Similar initiatives are being developed in other markets, such as the UK. For instance, the UK's Open Banking, a regulatory initiative that allows authorised third-party financial service providers to securely access consumer banking information,[14] has seen a rapid growth since it was introduced in 2018.[15] As of February 2022, over five million UK consumers and businesses have used open banking-enabled products, which are powered by extensive data and rigorous analysis.[16]

As it develops, the improving availability of data also lends support to global efforts to enhance financial inclusion. For instance, traditional commercial banks are generally more reluctant to grant loans or other forms of financing to SME clients, due in part to the intrinsic difficulty for businesses of smaller scale to meet the loan assessment requirements of banks. In the face of proliferation of business data, such may no longer be the case for SMEs, with alternative data starting to play a part in providing information to support alternative loan assessment methodologies. Data such as real-time supply chain transaction data, inventory and sales proceeds collected from the end consumer, payment history, cash flow, supply chain and number of employees, etc., can offer a 360-view of businesses – particularly of SMEs. This can be beneficial for bridging the gap by enabling the analysis of behavioural data rather than relying on traditional credibility measures of proof of income/revenue. Such usage of alternatives may encourage banks to provide more funding support to SMEs.

Data also plays a key role for risk management, by supporting the banking sector to monitor financial market activities and helping to detect illegal trading activities, such as money-laundering and fraudulent activities. Similarly, for the insurance sector, data analytics helps the sector to detect fraud as well as produce customer insights.

The power of data is exponentiated when synthesised from different sources, which is visible through dynamic ecosystems being formed between cross-industry entities. Taking RegTech as an example, these technologies are becoming increasingly dependent on high quality and high velocity data, which is often reliant on third parties that have the scale and capability to manage this data on behalf of multiple parties. Technological advancements in the field of artificial intelligence (AI) have also provided more channels for businesses of the financial services industry to meet various business needs by integrating AI into their operations. The power of data can also be magnified when its access is open and shared across different countries and borders, such as supporting multinational corporations to make better business decisions in various areas and helping countries fight against transnational crimes.

[14] UK Government, Corporate report: Update on Open Banking (5 November 2021), https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking (accessed on 16 June 2022)
[15] Open Banking, About the OBIE, https://www.openbanking.org.uk/about-us/ (accessed on 16 June 2022)
[16] UK Government, Corporate report: Update on Open Banking (5 November 2021), https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking (accessed on 16 June 2022)

Cross-boundary data flow to support the integration and digital transformation of the GBA

The GBA seeks to create a globally competitive ecosystem through integrating an international financial centre, a leading technology and innovation hub and other vibrant cities within the region with varied and mutually complementary advantages. The "Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area" (the Outline) issued by the State Council in 2019 emphasised the need to leverage the geographical advantages of the GBA to drive regional development, and highlighted a number of focus areas related to financial services industry, including (i) the development of cross-boundary financial services; (ii) the application of technology and innovation in fields including financial technologies and big data; (iii) and the prevention and mitigation of financial risks.[17]

Against this backdrop, enabling the frictionless cross-boundary flow of relevant financial data within the GBA is essential to fully implement these policy objectives. The key to integrated development lies in fostering the flow of people, goods, capital, and information. Having enhanced mechanisms to facilitate data exchange in a more timely, higher quality, and more effective manner is an integral part of its development.

In fact, market participants have longed for an effective flow of data within the GBA in order to accelerate their business expansion and integration within the region. Data-backed innovative technologies such as AI, blockchain, and big data are believed to be the solution to further enhancing the financial industry's capability to provide quality cross-boundary services to clients. Backed by such technologies, applications in digital identification, KYC procedures, risk evaluation and credit assessment, to list a few, can significantly improve customer experience and enable financial institutions to better serve SMEs and other traditionally underserved sectors.

Notably, such data-based innovation can also make a difference in reducing cyber risks and fraud cases at a local or regional scale as a large(r) dataset can help banks and other financial institutions to more effectively identify abnormal behaviours and irregular transaction patterns. Furthermore, with seamless data flow, businesses within the GBA can accelerate their digital adoption and continue to leverage AI to enhance business performance,[18] providing them with an additional competitive edge to flourish within the GBA and even internationally.

[17] HKSAR Government, Greater Bay Area, Outline Development Plan (18 February 2019), https://www.bayarea.gov.hk/filemanager/sc/share/pdf/Outline_Development_Plan.pdf (accessed on 16 June 2022)

[18] City University of Hong Kong, Legal research project: Proposal for Hong Kong To Be a Data Centre Hub For The Greater Bay Area and China (January 2019), https://www.cityu.edu.hk/slw/lib/doc/rccl/201901_RCCL_Report-HK_as_Data_Centre_Hub-ES.pdf (accessed on 16 June 2022)

Hong Kong should position itself to be the financial data hub for the GBA

Given the prominent role that data plays in supporting the development of the GBA, establishing a data hub that allows seamless data exchange within the GBA will unleash more potential of the power of data.

A data hub refers to the centre of data-related activities. The setup of a successful data hub could be driven by various factors, such as the increase of business activities that leads to the need for data and/or the production of data. With the data hub being formed, it provides data users with a centre point of access for data, allows data users to integrate and harmonise information from multiple sources, and also facilitates data flow.

In addition to being the leading international financial centre in this part of the world, Hong Kong, given its well-established IT infrastructure and strong research and innovation capabilities, should position itself to be the region's financial data hub to facilitate frictionless data flow. Notably, Hong Kong has a stable and extensive submarine cable communication network,[19] which is part of many submarine cable systems connecting other parts of Asia, Europe, and the US.[20] According to a data centre market study,[21] Hong Kong is ranked top in many of the 13 assessment categories for data centre markets, including market size, strong fibre connectivity, high cloud availability, market friendly tax regime, and rapid growing development pipeline for power. Overall, Hong Kong ranked second in Asia and sixth globally as a data hub, out of the 55 markets studied.

For smoother cross-border/boundary data flow to happen, it is important for the host of data to be well recognised as a trustworthy and secure place for data transmission and utilisation. In this regard, Hong Kong has been well regarded internationally – as a reputable and trustworthy city, with a strong governance structure and a vibrant business community. Such a reputation and its institutional setup has laid a strong foundation for Hong Kong to become a regional data hub and global digital financial centre.

Furthermore, the global trend of a data driven economy based on AI/big data development and the proliferation of digital media has increased the scale of data storage and transmission by tens of thousands. Notably, many countries have invested significantly in data infrastructure and have devoted resources to driving the development of digitalisation. Alongside the promotion of the digital economy, these countries have also introduced various data regulations and policies to enhance the legal framework for fostering healthy development of the industry. Therefore, it is important for Hong Kong to keep pace with global developments to remain competitive.

[19] Office of the Communications Authority, Landing of Submarine Cables in Hong Kong, https://www.ofca.gov.hk/en/industry_focus/infrastructures/submarine_cables/index.html (accessed on 2 February 2022)
[20] Submarine Cable Networks, Cabe Landing Stations in HK, https://www.submarinenetworks.com/stations/asia/hongkong (accessed on 5 January 2022)
[21] Cushman & Wakefield, 2022 Global Data Center Market Comparison (12 January 2022) https://cushwake.cld.bz/2022-Global-Data-Center-Market-Comparison (accessed on 5 April 2022)

In this regard, it is encouraging to see that the Hong Kong SAR Government has established a Digital Economy Development Committee (DEDC) in June 2022, among other initiatives, to support the development of its digital economy.[22] The DEDC is mandated to focus on various topics including setting strategies, enhancing cooperation with stakeholders, driving the growth of data services as an industry, encouraging the adoption of digitalisation by different industries, and promoting digital government.[23] More specifically, the DEDC has set up a sub-group on Cross-Boundary Data Collaboration, consisting of industry experts and other stakeholders, to identify, among others, possible approaches to facilitate cross-boundary data collaboration.[24]

With an aim of supporting the development of the GBA and Mainland China's digital economy, as well as implementing a related wider strategic plan,25 businesses expect Hong Kong to play a more significant role in data-related initiatives by leveraging its own unique advantages under "One Country, Two Systems".[26] If Hong Kong is able to facilitate data flow and enhance cross-boundary data availability between China and the rest of the world, data-oriented businesses will likely benefit from increasing opportunities to carry out more innovative product development and service enhancement.

[22] HKSAR Government, Government announces establishment of Digital Economy Development Committee (22 June 2022), https://www.info.gov.hk/gia/general/202206/22/P2022062200375.htm (accessed on June 25 2022)
[23] HKSAR Government, Government announces establishment of Digital Economy Development Committee (22 June 2022), https://www.info.gov.hk/gia/general/202206/22/P2022062200375.htm (accessed on June 25 2022)
[24] According to conversations with relevant public stakeholders.
[25] For instance, please see media report Wen Wei Po, "蔡冠深：港可為「數字絲路」發揮獨特作用" (5 March 2022), https://www.wenweipo.com/epaper/view/newsDetail/1499811929676451840.html (accessed on 5 April 2022)
[26] 2022 Foundation, Creating the Greater Bay Area of the Future – Opportunities for Hong Kong, http://www.2022foundation.com/images/GBA_MainReport.pdf (accessed on 5 April 2022)

Global data landscape and policies

For data to be shared and used safely and to drive value creation, it is essential that a practical and robust governance framework, covering the entire life cycle from data acquisition, storage, usage, processing, transferring, provision, and to disclosure, is in place. Given the GBA comprises three different legal systems and have different approaches to data governance, it will be useful to examine how data-related activities are regulated across different jurisdictions, particularly regarding cross-boundary data transfer. With that in mind, this section provides an overview of global approaches to cross-border/boundary data governance, with the focus on data polices of the United States, the European Union (EU), and Mainland China, as their approaches are considered representative of the main approaches adopted for data governance in the world.[27] An analysis of Hong Kong's data laws and approaches to international data transfers are also set out in this section.

Common mechanisms for cross-border/boundary data flows

Cross-border data transfer is governed based on several factors, including the policy objectives of the implementing jurisdictions. According to a 2019 white paper about data flow published by the World Economic Forum (WEF),[28] some common objectives that many jurisdictions consider while formulating related strategies are privacy protection, consumer protection, industry protection, economic stability, law enforcement, and national security.

Another key factor is the type of data – as some types of data have greater impact on and sensitivity to people, such as personal data or security-related data, understandably a higher level of discretion is warranted with regard to the transfer of such data. These categories are often subject to more legal restrictions – one of the most restrictive requirements is data localisation – under which data is required to be stored and/or processed in the country/region. In extreme situations, this can mean a complete ban on cross-border data transfers, even for the purpose of processing. In fewer extreme cases, jurisdictions may impose partial localisation, where data needs to be stored locally but transferring or storing copies of the data abroad is not prohibited.

The impact of data regulations on international data transfer varies, depending on the level of regulatory restrictiveness. That said, given the interconnectedness of businesses, many jurisdictions recognise the importance of international data transfers for businesses. This explains why countries generally allow the exporting of data, provided that data processors comply with specific regulatory requirements. These may include regulatory approval, various binding contracts, consent from data subjects, completion of a data protection-related assessment, among others. The five broad common mechanisms for international data transfers are summarised below.[29]

[27] World Economic Forum, Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence (December 2019), https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf (accessed on 2 March 2022)

[28] World Economic Forum, Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence (December 2019), https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf (accessed on 2 March 2022)

[29] Office of the Privacy Commissioner for Personal Data (PCPD), Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)

- **Whitelist:** data transfers are regulated on the basis of the data protection standards in the recipient country. Companies are allowed to export data to a receiving country if it is considered to have an adequate level of data protection as the hosting country, often referred to as an adequate jurisdiction. The most typical example would be the EU, which has recognised some countries as adequate jurisdictions, such as the three non-EU European Economic Area member countries.[30]

- **Safeguards:** data transfers across borders are allowed if contracts featuring model contractual clauses (also known as standard contractual clauses) pre-approved by regulators are signed between the sending and receiving parties. Many jurisdictions have implemented the mechanism of model contractual clauses for cross-border/boundary transfer. These include, for example, Hong Kong's Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (RMCs),[31] the EU's Standard Contractual Clauses (SCCs)[32] approved by the European Commission and ASEAN's Model Contractual Clause for Cross Border Data Flows (MCCs) developed by the Working Group on Digital Data Governance.[33] On 30 June 2022, Mainland China also issued a consultation paper on Standard Contractual Clauses for cross-border personal information transfer, and the consulting period ended on 22 July 2022.[34]

- **Certifications:** companies are allowed to transfer and receive data from certain jurisdictions if certain certifications related to data privacy protection are obtained from a professional body recognised by regulators. For example, Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) system is a voluntary and accountability-based system that consists of a series of internationally recognised data privacy protection standards. A company certified under the CBPR system is allowed to transfer and receive personal data collected in an APEC member economy across borders.[35] One data privacy protection standard included in the CBPR system is the APEC Privacy Framework, which is designed to protect privacy while ensuring personal information is able to flow freely to benefit consumers, businesses, and governments.[36]

[30] Namely Iceland, Liechtenstein and Norway.
[31] PCPD, "Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data" (May 2022), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf (accessed on 6 June 2022)
[32] European Commission, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on 4 March 2022)
[33] Personal Data Protection Commission of Singapore, ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows (January 2021), https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows (accessed on 4 March 2022)
[34] Cyberspace Administration of China,《个人信息出境标准合同规定(征求意见稿)》(30 June 2022), http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm (accessed on 24 October 2022)
[35] APEC, What is the Cross-Border Privacy Rules System (October 2021), https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system (accessed on 6 June 2022)
[36] Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework (August 2017), https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (accessed on 6 June 2022)

- **Necessity:** most jurisdictions prohibit the international transfer of (personal) data by default, and only permit the transfer of such data for certain purposes, such as for business needs (e.g., a performance of a contract). Notably, necessity is often a prerequisite for an international data transfer.

- **Consent:** some jurisdictions require data users to obtain consent from data subjects (e.g., natural persons) prior to the transfer of personal data. Nonetheless, the level of consent required may vary across markets. For instance, Mainland China requires express consent from data subjects to proceed for every transfer,[37] whereas in Hong Kong, consent from data subjects is needed only if the transfer is initiated for a new purpose.[38]

Furthermore, jurisdictions may adopt more than one mechanism for the transfer of data across boundaries, especially for handling personal data. For example, in Mainland China, data users are required to obtain a consent plus a government approval, a certification, or a contract with the data recipient, among others, before a transfer of personal data can take place. Comparatively, some rare jurisdictions are bound by less legal requirements for the transfer of personal data. For example, in the Republic of Korea, companies are only required to obtain consent from data subjects prior to exporting personal data. Whereas for cases that involve cross-border data interchange, apart from the above legal requirements, data users are expected to take into account fundamental data principles as they would be required to for cases of local data transfer, such as data needing to be collected for a lawful purpose.

The United States

According to a UN study on the digital economy,[39] the United States has adopted a free-market approach towards the digital economy, which enables cross-boundary free flow of data. Such proposition favours a private market-driven approach that stimulates innovation and supports first-mover advantages, and, as a result, technology companies in the United States have arguably achieved a dominant position comparatively. The United States has used trade agreements to enable firms to gain access to foreign markets and ban practices such as data and server localisation requirements. This approach enables data to flow back to the United States when overseas users engage with firms headquartered in the country.

The UN study notes that the United States does not impose any specific compliance requirements for cross-boundary transfers of personal data. It has, however, taken a restrictive approach for data related to defence and national security issues, such as requiring any company providing cloud services to its defence department to store its data only in the United States.[40]

---

[37] The National People's Congress of the People's Republic of China,《中华人民共和国个人信息保护法》(20 August 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed 2 December 2021)
[38] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)
[39] UNCTAD, Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)
[40] UNCTAD, Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)

For data privacy, it has opted for a flexible and ad-hoc sectoral approach, and only prescribed standards in specific areas such as child privacy, health information, and financial data privacy. While none of these sectoral regulations restrict cross-boundary data transfer, these sectors are subject to more restrictive compliance requirements. Take the financial services industry as an example, the United States has imposed a range of personal and financial data regulations to ensure market efficiency, consumer protection, and financial stability alongside the flow of data.[41]

The UN study argues that the United States has adopted such a liberal regulatory approach on cross-boundary data flow to maintain and further expand its leadership in the global digital market. Therefore, it has advocated against data protectionism and supports cross-border data governance, such as endorsing the APEC Privacy Framework and APEC's CBPR system.

The EU

According to the European Data Strategy published by the European Commission (EC) in February 2020, the EU aims to "create a single market for data", where data with the EU can flow freely with respect to European rules, including privacy and data protection as well as competition law.[42]

The EU's data policy is mainly governed by the General Data Protection Regulation (GDPR), which is widely recognised as one of the most comprehensive data protection frameworks in the world. In general, the EU takes a strong regulatory approach towards the digital economy, which is formulated based on the protection of fundamental rights and values of the EU.[43] Regulations on cross border data flow are relatively more stringent with an aim of protecting the privacy of individuals. While the governance with regard to the transfer of personal data outside of the region is challenging, the EU does not explicitly ban the exit of non-personal data.

Under the GDPR, transfer of personal data outside of the EU is only allowed if the recipient countries reciprocally provide a similar level of privacy protection to its citizens as the EU, as designated by the EC. As of 17 March 2022, countries or territories that the EC has endorsed as having an adequate level of privacy protection to its citizens are Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom.[44,45]

Another mechanism to enable international transfer is to adopt appropriate safeguards (such as standard contractual clauses [SCCs] approved by the EC or binding corporate rules [BCRs] for intragroup transfers) and the data subjects should possess enforceable rights and be protected by effective legal remedies. In the absence of an option under the two approaches mentioned before, transfer of personal data is still possible if the action falls under a derogation (exception) specified in the GDPR (e.g., explicit consent of the data subjects, or if necessary, to exercise or defend a legal claim, amongst others).[46]

---

41 SSRN, Financial Data Governance: The Datafication of Finance, the Rise of Open Banking and the End of the Data Centralization Paradigm by Douglas W. Arner, et al (23 March 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4040604 (accessed on 4 Ap ril 2022)

42 European Commission, The European Data Strategy (19 February 2020), https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283 (accessed on 4 April 2022)

43 UNCTAD, Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)

44 The adequacy findings is a product of long bilateral negotiations, with the EU taking into considerations of several factors of the negotiating parties, including their data protection framework, legal system, and their economic and political relationship with the EU.

45 European Commission, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed on 3 February 2022)

46 In July 2020, the ECJ ruled in Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 that the EU-US Privacy Shield mechanism for international transfers was invalid and that, if companies are looking to rely on SCCs to enable a transfer of personal data outside the EEA, entities must carry out an evaluation to determine if the recipient country's laws undermines the ability of the SCCs to provide the GDPR's required level of data protection. As such, supplementary measures may also need to be implemented to ensure the transferred data is adequately protected.

Mainland China

In Mainland China, approaches for the flow of cross-border/boundary data are incorporated in several laws. They are mainly regulated by the Data Security Law (implemented on 1 September 2021),[47] Personal Information Protection Law (implemented on November 1, 2021),[48] and the Cyber Security Law (implemented on 1 June 2017),[49] among others.[50] As suggested by the names of these regulations, Mainland China's data regulations explicitly govern aspects beyond just personal data.

Data Security Law

Mainland China's Data Security Law (DSL) became effective in September 2021, with the purpose of "regulating data processing, ensuring data security, promoting development and utilisation of data, protecting the lawful rights and interests of individuals and organisations, and safeguarding the sovereignty, security, and development interests of the state".[51]

Articles 11 and 31 of the DSL provide the conditions for cross-border/boundary data transfer.[52] Article 11 is a principal provision, highlighting the country's support for promoting cross-border/boundary data. Article 11 stipulates that the Mainland government will actively carry out international exchanges and cooperation in the fields of data security governance, data development and utilisation, participate in the formulation of international rules and standards related to data security, and facilitate the safe and free flow of cross-border/boundary data.

Article 31 stipulates that the exit security management of important data collected and generated by operators of critical information infrastructure during operations within the territory of Mainland China shall be governed by the provisions of the Cyber Security Law in conjunction with relevant departments of the State Council.

[47] The National People's Congress of the People's Republic of China,《中华人民共和国数据安全法》(10 June 2021), http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (accessed 2 December 2021)
[48] The National People's Congress of the People's Republic of China,《中华人民共和国个人信息保护法》(20 August 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed 2 December 2021)
[49] Cyberspace Administration of China,《中华人民共和国网络安全法》(7 November 2016), http://npc.people.com.cn/n1/2016/1124/c14576-28892612.html (accessed 2 December 2021)
[50] Please refer to the Appendix for a summary of Mainland China's data regulations development.
[51] The National People's Congress of the People's Republic of China, Data Security Law of the People's Republic of China (10 June 2021), http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm (accessed on 5 March 2022)
[52] The National People's Congress of the People's Republic of China,《中华人民共和国数据安全法》(10 June 2021), http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (accessed 2 December 2021)

Personal Information Protection Law

Mainland China imposes data localisation of personal data and restricts the exit of personal data.[53] The Personal Information Protection Law (PIPL) provides special chapters on cross-border/boundary provision of personal information - Article 38 stipulates that personal information processors should only provide personal information outside Mainland China due to business needs; PIPL requires separate consent from subjects for personal data to be transferred out of Mainland China (article 39 & 55 of PIPL). Additionally, one of the following conditions should be fulfilled:

i. passing the security assessment organised by the Cyberspace Administration in accordance with Article 40 of PIPL;

ii. obtaining personal information protection certification by a professional organisation pursuant to the provisions of the Cyberspace Administration;

iii. concluding a contract with the overseas entities, according to the standard contract formulated by the Cyberspace Administration, to stipulate the rights and obligations of both parties;

iv. complying with other conditions stipulated by laws, administrative regulations or the Cyberspace Administration.

Where the international treaties and agreements that Mainland China has concluded or participated in have provisions on the conditions to provide personal information outside of the Mainland, cross-border/boundary transfer of personal information can be implemented in accordance with those provisions. Personal information processors shall take necessary measures to ensure that the processing of personal information by overseas recipients meets the personal information protection standards stipulated in this law.

Cyber Security Law

The cross-border/boundary provisions for critical infrastructure data are stipulated in the Cyber Security Law (CSL). According to the CSL, "the personal information and important data collected and generated by operators of critical infrastructure during operations within the territory of Mainland China shall be stored in Mainland China".[54]

[53] The National People's Congress of the People's Republic of China,《中华人民共和国个人信息保护法》(20 August 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed 2 December 2021)

[54] The term "critical infrastructure" is defined to include "public communications services, energy, transport, water conservation, finance, public services, e-government affairs or anything else where data loss, destruction or leakage can result serious damage to state security, national economy and people's livelihood and public interests" Please see Cyberspace Administration of China,《中华人民共和国网络安全法》(7 November 2016), http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm (accessed 2 December 2021)
UNCTAD, Digital Economy Report 2021 (March 2022), https://unctad.org/webflyer/digital-economy-report-2021 (accessed on 5 March 2022)
Cyberspace Administration of China,《中华人民共和国网络安全法》(7 November 2016), http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm (accessed 2 December 2021)

With an aim of ensuring public security and easy access to data for regulatory purposes, Mainland China imposes data localisation for information of several specific sectors, including health and/or personal information collected by credit investigation organisations, commercial banks, internet map service organisations, online taxi platform companies, and internet bicycle rental operators.[55] When it is necessary to provide data to overseas recipients due to business needs, "a security assessment shall be carried out in accordance with the measures formulated by the Cyberspace Administration in conjunction with relevant departments of the State Council."[56]

Given the importance of security assessment in data exportation for Mainland China, it is worth mentioning that in July 2022, the Cyberspace Administration issued the "Data Outbound Security Assessment Measure" (the Measure), which specifies rules and procedures for the implementation of the security assessment for cross-border/boundary data transfer as stipulated in the Data Security Law, Personal Information Protection Law, and Cyber Security Law.[57] Subsequently, the "Data Outbound Security Assessment Declaration Guidelines" was published in August,[58] providing more guidance on the application method, process, supporting documents, and other means required for the security assessment. According to the Measure, specific players[59] will have to register for a security assessment prior to transferring data overseas.

In general, at present, the exit of both personal information and important data (i.e., collected by operators of critical information infrastructure or operators of other data processors) must undergo strict security assessment, certification, or standard contract review.

Cross-border/boundary data flow arrangements in Free Trade Zones and the GBA

Given the strong demand for cross-border/bounda ry data flow and many legal restrictions on the provision of cross-border/boundary data, free trade zones in Hainan, Shanghai, and Beijing, namely Hainan Free Trade Port,[60] Shanghai Lingang Area,[61]and Beijing Digital Trade Pilot Zone,[62] rely on their respective policy supports to explore solutions for cross-border/boundary data flow based on their regional industrial development needs.

[55] People's Republic of China, Cyberspace Administration of China, "數據出境安全評估辦法" (7 July 2022), http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (accessed on 15 July 2022)
[56] Cyberspace Administration of China, 國家互聯網信息辦公室發布《數據出境安全評估申報指南（第一版）》(31 August 2022), http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm (accessed on 9 September 2022)
[57] People's Republic of China, Cyberspace Administration of China, "數據出境安全評估辦法" (7 July 2022), http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (accessed on 15 July 2022)
[58] Cyberspace Administration of China, 國家互聯網信息辦公室發布《數據出境安全評估申報指南（第一版）》(31 August 2022), http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm (accessed on 9 September 2022)
[59] These players include data processors transferring important data abroad, operators of critical information infrastructure, data processors handling the personal information of over 1 million users, and data processors who have either accumulatively provided the personal information of over 100,000 users or sensitive information of over 10,000 users abroad since January 2021.
[60] The People's Republic of China, 中共中央国务院印发海南自由贸易港建设总体方案 (1 June 2020), http://www.gov.cn/zhengce/2020-06/01/content_5516608.htm (accessed on15 February 2022)
[61] People's Government of Shanghai, 上海市人民政府关于印发《上海市全面深化服务贸易创新发展试点实施方案》的通知 (5 November 2020), https://www.cs.com.cn/xwzx/hg/202011/t20201113_6111251.html (accessed on 25 February 2022)
[62] The People's Government of Beijing Municipality, 北京市商务局关于印发《北京市关于打造数字贸易试验区实施方案》的通知 (18 September 2020), http://www.beijing.gov.cn/zhengce/zhengcefagui/202009/t20200923_2088196.html (accessed on 16 June 2022)

These policies and measures provide useful references for the GBA. On cross-border/boundary data governance, various attempts are being explored in the free trade zones, aiming to leverage their respective policy advantages to achieve breakthroughs in the following five key aspects:

1. Carrying out **pilot projects** for cross-border/boundary data transmission security management. For example, Hainan proposes to explore more convenient methods with a view to conducting assessments for the secure exit of personal information.[63]

2. Carrying out a **security assessment** of cross-border/boundary data flow and **building a public service platform** to facilitate the flow.[64]

3. For **specific industries**, such as the financial sector, allowing eligible foreign financial institutions to report and transfer relevant data overseas due to a group's holding of financial institutions in Mainland China. Relevant data could include those regarding internal management and risk control, according to the cross-border/boundary data classification supervision model proposed by Shanghai.[65]

4. For **specific companies**, as proposed by Beijing Digital Trade Pilot Zone, actively promoting a small number of pilot companies in the pilot zone to achieve data flow compliance within specific areas abroad.[66]

5. Supporting **international collaboration**, with China-Japan-Korea, ASEAN, and other regional blocs as a start, expanding to the US and the EU for cross-border data transfer.[67]

On 5 September 2021, Mainland China issued the "Overall Plan for the Construction of the Hengqin Guangdong-Macao Intensive Cooperation Zone" (the Plan), which provides some visions for safe and orderly cross-border/boundary transfer of data.[68]

The Plan states that under the national security management framework for cross-border/boundary data transmission, relevant authorities will carry out pilot projects for cross-border/boundary data transmission, study the construction of green channels for a fixed network to access the worldwide internet, and explore the formation of a mechanism that can facilitate data flow while ensuring security. It will also support relevant universities and scientific research institutions in Zhuhai and Macao to achieve the interconnection of cross-border/boundary scientific research data under the condition that personal information and important data are secured.

---

[63] The People's Republic of China, 中共中央国务院印发海南自由贸易港建设总体方案 (1 June 2020), http://www.gov.cn/zhengce/2020-06/01/content_5516608.htm (accessed on 15 February 2022)

[64] People's Government of Shanghai, 上海市人民政府关于印发《上海市全面深化服务贸易创新发展试点实施方案》的通知 (5 November 2020), https://www.cs.com.cn/xwzx/hg/202011/t20201113_6111251.html (accessed on 25 February 2022)

[65] People's Government of Shanghai, 上海市人民政府关于印发《上海市全面深化服务贸易创新发展试点实施方案》的通知 (5 November 2020), https://www.cs.com.cn/xwzx/hg/202011/t20201113_6111251.html (accessed on 25 February 2022)

[66] The People's Government of Beijing Municipality, 北京市商务局关于印发《北京市关于打造数字贸易试验区实施方案》的通知 (18 September 2020), http://www.beijing.gov.cn/zhengce/zhengcefagui/202009/t20200923_2088196.html (accessed on 16 June 2022)

[67] The People's Government of Beijing Municipality, 北京市商务局关于印发《北京市关于打造数字贸易试验区实施方案》的通知 (18 September 2020), http://www.beijing.gov.cn/zhengce/zhengcefagui/202009/t20200923_2088196.html (accessed on 16 June 2022)

[68] The People's Republic of China, 中共中央国务院印发《横琴粤澳深度合作区建设总体方案》(5 September 2021), http://www.gov.cn/zhengce/2021-09/05/content_5635547.htm (accessed on 30 May 2022)

Hong Kong

Hong Kong's main data regulation is the Personal Data (Privacy) Ordinance (PDPO), whose primary concern is personal data and privacy protection. PDPO defines personal data as information which relates to a living individual and can be used to identify that individual. It must also exist in a form which access to or processing of, is practicable.[69]

Notably, Section 33 of PDPO is intended to be the guiding principle for cross-border/boundary transfer of data under Hong Kong's existing legal framework. However, due to concerns from the business community over its potential impact on business operations and compliance difficulties,[70] the section has not been implemented, despite its introduction in 1996.

Cross-border/boundary data transfer arrangements

Section 33 of the PDPO sketches out under what circumstances personal data can be gathered within Hong Kong and the conditions that need to be met before cross-border/boundary data transfer is allowed.

- s33(2)(a) Jurisdictions with data privacy protection laws that are same or similar as those in Hong Kong (i.e., PDPO), which have been confirmed by the Privacy Commissioner for Personal Data through the publication by notice in the Gazette;
- s33(2)(b) If the user has reasonable grounds to believe that the jurisdiction has any law that is similar to the PDPO in Hong Kong;
- s33(2)(c) Data subject has given written consent for the transfer;
- s33(2)(d) For the benefit of the person's with the personal data (subject to more detailed stipulations);
- s33(2)(e) Other exceptions.

As section 33 of PDPO is not in effect, there is technically no specific law governing the cross-border/boundary transfer of data in Hong Kong. That said, six Data Protection Principles[71] (DPP) are in place to guide the collection and usage of personal data. For the purpose of cross-border/boundary data transfer, such principles include:

- DPP 2(3) requires data users to prevent their processors from retaining personal data longer than necessary, and
- DPP 3 prohibits transfer of personal data for new purposes without consent.

---

[69] PCPD, The Personal Data (Privacy) Ordinance, https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html (accessed on 15 December 2021)

[70] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)

[71] HKSAR Government, Personal Data (Privacy) Ordinance (last updated on 8 October 2021), https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y (accessed on 7 February 2022)

- DPP 4(2) requires data users to ensure that the security of personal data transferred to their processors are all applicable to cross-border/boundary data usage.

    - Furthermore, under section 65(2) of the PDPO, data users are liable for the acts of their agents, which can be used to cover the acts of overseas service providers as well. As such, data users who may transfer data collected in Hong Kong to overseas service providers can still be held liable should anything go amiss.

Other than the mechanisms stipulated in the DPP and PDPO, it is also possible to establish contractual obligation on overseas parties regarding how they handle personal data obtained within Hong Kong. The PCPD has issued the Recommended Model Contractual Clauses for the Cross-border Transfer of Personal Data (RMCs), which are free-standing clauses that may be incorporated into business agreements between transferors and data transferees across borders/boundaries.[72] Such clauses aim to help businesses to take into consideration the relevant requirements of data protection set out in the PDPO. An example on a wider scale will be bilateral agreements between jurisdictions, whereby there may still be jurisdictional applicable rules/commitment to cross-border data transfer. In the bilateral free trade agreement (FTA) between Hong Kong and Australia from 2019, a declaration of commitments to the policy of free flow of data was included in the FTA. Remarkably, approaches in Hong Kong are in line with the approaches of other jurisdictions, such as the EU and Mainland China.

We are also aware that the Government is formulating regulations that define the cyber security obligations of critical infrastructure operators,[73] which may impact the relevant operators. A public consultation exercise is expected to be launched by the end of 2022 and the FSDC will continue to monitor this space.

[72] PCPD, "Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data" (May 2022), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf (accessed on 6 June 2022)

[73] HKSAR Government, "Cyber security legislation proposed" (25 May 2022), https://www.news.gov.hk/eng/2022/05/20220525/20220525_125433_066.html

Pain points facing Hong Kong's financial services industry

The financial services industry in the GBA has become increasingly integrated in recent years, with the latest milestone being the launch of the Wealth Management Connect in 2021[74] and the ETF Connect in July 2022.[75] In contrast, connectivity in respect of financial data seems to be lagging, posing operational challenges and compliance uncertainties for businesses operating across the GBA.

Lack of specific legislation to facilitate cross-border/boundary data transfers

There is a lack of specific legislation to facilitate data transfer in Hong Kong. Section 33 of the PDPO prohibits the transfer of personal data to places outside of Hong Kong unless one of the specified conditions is fulfilled.[76] That said, it has not been in force since the PDPO took effect from December 1996. While the Office of the Privacy Commissioner for Personal Data (PCPD) has in the past commissioned consultancy studies on bringing section 33 into force, it remains unclear when the particular statutory provision will be effective.[77] According to a PCPD document, seven issues related to the implementation of section 33 were raised from a study, ranging from definition, implementation, and enforcement to policy interaction with other regulations governing certain highly regulated industries.[78]

Concerns from businesses about the impact on their operations, compliance difficulties, and additional time and effort required in relation to these, have led to the implementation of section 33 being deferred.[79] For example, as stated in the aforementioned PDPO document, if a jurisdiction was previously confirmed by the PCPD as having the same or similar data protection laws as those in Hong Kong (i.e., the PDPO), but is later delisted by the Commissioner as one which is no longer considered to have a similar law as the PDPO, the steps that a business should take to ensure their compliance with the law is uncertain.[80]

[74] HKMA, Cross-boundary Wealth Management Connect Scheme in the Guangdong-Hong Kong-Macao Greater Bay Area (9 November 2021), https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/wealth-management-connect/ (accessed on 23 March 2022)
[75] Hong Kong Exchanges and Clearing Limited (HKEX), "HKEX to Include ETFs in Stock Connect on 4 July" (28 June 2028), https://www.hkex.com.hk/News/News-Release/2022/220628news?sc_lang=en (accessed on 30 June 2022)
[76] PCPD, Response to media enquiry on data localisation (15 April 2020), https://www.pcpd.org.hk/english/news_events/media_enquiry/enquiry_20200415.html (accessed 2 April 2022)
[77] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)
[78] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)
[79] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)
[80] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)

The changing regulatory landscape of data protection

The recently legislated/imposed data laws in Mainland China have distinctive impacts on cross-boundary data governance and may have far-reaching implications for Hong Kong. One of the foundations of Hong Kong's role as an international financial centre of China and part of the GBA is its strong connection with Mainland China in various aspects, including people, business, and other social interactions. In this regard, while protecting the interests of data subjects, the frictionless flow of data between Hong Kong and Mainland China is essential to fostering strong connectivity. Nevertheless, as Hong Kong is considered an "offshore" market of Mainland China with its own legal system under "One Country, Two Systems", a higher degree of policy coordination will be needed to facilitate more effective cross-boundary data activities.

Having compared the data laws in Mainland China and Hong Kong, both jurisdictions share some common data protection principles. For instance, according to articles 5 to 8 of Mainland China's PIPL, the collection and handling of personal information shall, but not limited to, "follow the principles of lawfulness, legitimacy, necessity, and integrity"; "follow the principles of openness and transparency";[81] "have a clear and reasonable purpose", and "guarantee the quality of personal information". According to Hong Kong's six Data Protection Principals, Principle 1 requires personal data, but not limited to, shall be collected "for a lawful purpose", "by means which are lawful and fair in the circumstances of the case"; Principle 2 requires, but not limited to, "all practicable steps shall be taken to ensure that personal data is accurate having regard to the purpose for which the data is or is to be used".[82]

While there are similarities in data protection principles between the two jurisdictions,[83] legal requirements to ensure data protection are different. They have discrete legal requirements to ensure data protection. Notably, Mainland China requires operators of critical information infrastructure and entities which process personal information beyond the limits determined by the Cyberspace Administration of China to store data locally, whereas Hong Kong's PDPO does not impose such data localisation requirement on any specific data processors. Indeed, this might change after the Government has enacted the laws in relation to defining obligations of critical infrastructure operators,[84] which may have an impact on relevant operators.

[81] The National People's Congress of the People's Republic of China,《中华人民共和国个人信息保护法》(20 August 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed on 2 December 2021)

[82] HKSAR Government, Personal Data (Privacy) Ordinance (last updated on 8 October 2021), https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y (accessed on 7 February 2022)

[83] PCPD, Six Data Protection Principles, https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/files/6DPP.pdf (accessed on 30 May 2022); The National People's Congress of the People's Republic of China,《中华人民共和国个人信息保护法》(20 August 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed 2 December 2021)

[84] HKSAR Government, "Cyber security legislation proposed" (25 May 2022), https://www.news.gov.hk/eng/2022/05/20220525/20220525_125433_066.html (accessed on 7 July 2022)

Additionally, the main data laws of Mainland China were introduced within the last five years and guidance on specific aspects is still being formulated. This gives rise to unintended uncertainties, resulting in many organisations adopting a "play it safe" approach and putting in place restrictions beyond the original legislative intent. For example, Mainland China's DSL, which came into effect in 2021, requires a higher level of protection to "critical data" without further clarifying its definition. Subsequently, in January 2022, the draft of "Information security technology – Guideline for identification of critical data" published by the State Administration for Market Regulation and Standardisation Administration preliminarily defined "critical data" as the type of data that can cause harm to national security and public interests, if it is modified, destroyed, leaked, or illegally obtained and used.[85]

While the draft of "Information security technology – Guideline for identification of critical data" is yet to be finalised, the definition of "critical data" as mentioned above has been adopted by the "Measure".[86] Many law firms have underlined that guidance on the definition of "critical data" and identifications of similar types of data will require clarity and certainty.[87]

According to a news report, due to uncertainties around data protection requirements, particularly related to cross-border/boundary data transfers, some foreign businesses decided to scale back their planned budget for research and development projects in Mainland China, while some other businesses were compelled to downgrade the quality of service provided to clients.[88]

It will take time for the financial services industry, as with other economic sectors, to observe and understand the implementation of the series of updates around data governance in Mainland China, and the relevant implications on cross-boundary data transmission as related to business needs. For the time being, these policy changes while necessary to ensure data protection, will unavoidably bring about some level of uncertainty to the integration of cross-boundary financial services.

Operational obstacles

Insufficient data integration within the GBA has created many operational obstacles for GBA companies. Businesses face difficulties in fulfilling Know-Your-Customer ("KYC") compliance, obtaining alternative data source of credit rating, etc., when promoting the financial services across the GBA regions. For example, banks in Hong Kong may not be able to obtain KYC information from banks in Mainland cities, due to the cross-boundary data privacy protection and conflicting cyber security laws and vice versa.

[85] National Information Security Standardization Technical Committee,《信息安全技術重要數據識別指南》(7 January 2022), https://www.tc260.org.cn/file/2022-01-13/bce09e6b-1216-4248-859b-ec3915010f5a.pdf (accessed on 7 July 2022)
[86] People's Republic of China, Cyberspace Administration of China, "數據出境安全評估辦法" (7 July 2022), http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (accessed on 15 July 2022)
[87] IFLR, "PRIMER: China's Data Security Law" (11 November 2021), https://www.iflr.com/article/2a6478kz8k2ue7ln620ao/primer-chinas-data-security-law (accessed on 28 June 2021)
[88] SCMP, "China must clarify 'uncertainty' over data security laws, allow more cross-border transfers" (23 November 2021), https://www.scmp.com/economy/china-economy/article/3157026/china-must-clarify-uncertainty-over-data-security-laws-allow (accessed on 30 June 2022)

Another example is the validation of letters of guarantees. Currently there is no centralised database where financial institutions, banks and FinTech incumbents can share their customers' credit reports and collateral.[89] Companies will also have difficulty finding a trusted notary across boundaries to validate and value collaterals.

Companies with operations in Mainland China and Hong Kong are struggling to integrate their businesses. For example, under the current arrangement, any Mainland subsidiary of a Hong Kong-based company must meet a set of legal requirements for transferring company data to Hong Kong. Hence, a business might hesitate to conduct cross-boundary data transfer, thereby hindering business integration.

Encouragingly, there have been developments in the GBA to address challenges of cross-boundary customer onboarding in the banking sector. In November 2021, Guangzhou launched the Greater Bay Area Cross-border Data Mutual Recognition Platform, which allows banks to verify the identities of customers residing in Guangdong and Hong Kong, therefore making the cross-boundary KYC checks more effective.[90] That said, more effort will be required to overcome the operational challenges mentioned above.

Compliance cost and challenges

The lack of an integrated framework governing data transfer within the region means that businesses must consider how to coordinate between all the data laws and understand conflicting cases, if any, and, if so, how to resolve them. The cost to meet legal requirements for cross-boundary transfer of data (such as personal data or operational data) to take place within the region is significant and felt even more acutely by SMEs, which have limited capital and resources to invest in legal and compliance.

The compliance challenges have also deterred banks from onboarding SME clients as they generally have less collateral or credit-related data to meet the lending requirements of financial institutions. As mentioned before, using alternative data can be a solution to promote financial inclusion, enabling underserved SMEs to have greater access to financial support.

[89] Nova, 实现跨境企业征信建设跨境信用机制诺华诚信参与草拟跨境企业信用标准 (20 December 2021), https://www.nova-credit.com/zh-hans/news/detail/49/ (accessed 23 January 2022)

[90] The People's Government of Guangzhou Municipality, 广州南沙建大湾区跨境数据互信互认平台 (6 December 2021), http://www.gz.gov.cn/ysgz/xwdt/ysdt/content/post_7947573.html (accessed on 17 December 2021)

Talent shortage

In order to stay at the forefront of the evolution, businesses rely on their workforce to design, execute, and review their data and digitalisation strategies. However, Hong Kong businesses are confronted with talent scarcity. A relatively small talent pool in the information technology industry has long been one of the challenges facing Hong Kong's technology and data sector. According to the Talent Development Survey 2021 conducted by the Hong Kong Institute of Bankers, 82% of surveyed financial industry practitioners considered technological and data skills as the greatest skill gap for the banking industry. There is no surprise that innovation and technology experts, data scientists and cyber security specialists, and Fintech professionals are three of the 13 professions in the Talent List of Hong Kong that the city seeks to attract.[91]

In particular, companies have expressed their struggles to find talent that has both data-related competency and business sense. For example, according to a 2021 study of a consulting firm, 40% of Hong Kong companies surveyed indicated the "lack of talent with integrated knowledge in technology and management" as one of the top three challenges that hinder their technological innovation.[92] Given the increasingly sophisticated business needs, companies not only expect data scientists to be technically sound, but also to have a nuanced business sense in analysing huge datasets to help companies navigate critical business decisions. It can be challenging for data talent who are well-versed in computer science and statistics to understand the business landscape, especially the more complicated overlays of implicit business rules and processes.

Additionally, businesses are also experiencing challenges to acquire and nurture home-grown and foreign talent. While the information technology industry is gaining greater attention and wider popularity among university students, there is still a considerable gap between Hong Kong graduates' skillsets and the demands of workplaces.[93] It is therefore important for students to find theories and skills taught in the classroom to be highly relevant and practical in the work environment, especially as technology is continuing to evolve rapidly across various industries. Many companies have also quoted their challenging process to retain and source foreign talent to fill the local demand gap, especially for senior-level talent.[94]

Talent shortage in Hong Kong across various industry sectors is further highlighted by the ongoing COVID-19 pandemic.[95] While the supply of talent has decreased, the demand for data talent has increased dramatically since industry players have been racing against each other to accelerate their digitalisation agenda during this period.

---

91 HKSAR Government, The 13 Professions on the Talent List, https://www.talentlist.gov.hk/en/talentlist.html (accessed on 15 July 2022)

92 Deloitte, Rekindling Hong Kong's economic growth through innovation (December 2021), https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-2021-hk-techfast-announced-en-20211210.pdf (accessed on 15 July 2022)

93 SCMP, "Hong Kong's IT sector facing shortage of skilled talent as Covid-19 keeps foreigners away and locals mull migration" (13 March 2021), https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3125233/hong-kongs-it-sector-facing-shortage-skilled (accessed on 15 July 2022)

94 Ming Pao, "獵頭公司：主要外籍人才流失 5年內港成不吸引城市" (31 March 2022), https://news.mingpao.com/pns/%E6%B8%AF%E8%81%9E/article/20220331/s00002/1648663924393/%E7%8D%B5%E9%A0%AD%E5%85%AC%E5%8F%B8-%E4%B8%BB%E8%A6%81%E5%A4%96%E7%B1%8D%E4%BA%BA%E6%89%8D%E6%B5%81%E5%A4%B1-5%E5%B9%B4%E5%85%A7%E6%B8%AF%E6%88%90%E4%B8%8D%E5%90%B8%E5%BC%95%E5%9F%8E%E5%B8%82 (accessed 15 July 2022)

95 SCMP, "Hong Kong's banking talent shortage worsened by zero-Covid rules must be urgently addressed, industry association says" (21 January 2022), https://www.scmp.com/business/banking-finance/article/3164299/hong-kongs-banking-talent-shortage-worsened-zero-covid (accessed 15 July 2022)

Policy recommendations

In order to achieve an effective flow of financial data within the GBA, and to position Hong Kong's role as the financial data hub of the region, this report proposes some recommendations in the following aspects.

To provide clarity on section 33 of PDPO

As mentioned previously, PDPO is the major legislation in Hong Kong that is related to data governance. While its section 33 governs the transfer of personal data from Hong Kong to other jurisdictions, it has not been implemented since its introduction in 1996 due to concerns from businesses over its operational impact and compliance difficulties.[96] The six Data Protection Principles has become one of the key guidelines for handling personal data across borders/boundaries. Nonetheless, these principles focus on personal data protection, with limited clarity and guidelines on ways to carry out cross-border data transfers than section 33, if it was implemented.[97] Hence, a clear legal framework that spells out mechanisms can facilitate international data transfers. Additionally, it also demonstrates a jurisdiction's adequacy of data protection. In this context, Hong Kong, with an aim of taking up the role as a facilitator of safe and secure flow of data across the region, should provide clarity on relevant rules and regulations in the data space.

In this respect, the industry has been seeking clarity on the PDPO, particularly regarding section 33. A clear timeline about the implementation of section 33 will be crucial for establishing a legal framework for GBA integration. Understandably, businesses should be given sufficient time to implement the necessary measures to comply with the data laws. The Government should therefore consider setting up a roadmap in relation to the implementation, with an objective to address the previously mentioned challenges. This includes how businesses can remain compliant with the law if a jurisdiction that was initially approved by the Commissioner for international data transfer was delisted by the Commissioner afterwards.

To foster the development of an orderly and healthy market, it is important that rules and regulations keep pace with technological and commercial realities, with defined requirements and standards clearly laid out. This would lead to appropriate regulations on parties involved in data exchange, thereby ensuring the accuracy, validity, and security of data. Notably, laws of section 33 that govern data transfer were first created decades ago, before the mass scale of data was being utilised for personal and commercial purposes as it is today. Therefore, prompting a need to review and potentially update the rules is necessary to ensure they remain fit for purpose prior to the formulation of a timeline and roadmap.

Looking ahead, it is worth considering mandating companies of a certain scale, or companies handling large amounts of personal and/or sensitive data, to designate a data protection officer (DPO) to take on the responsibility of ensuring their organisations comply with all the relevant data laws.

Such a practice has become the norm in many jurisdictions, including the EU.[98] At the same time, the PCPD has also advocated the inclusion of a DPO as part of organisations' data governance in the best practice guide issued under the Privacy Management Programme.[99] However, to demonstrate that Hong Kong is well-positioned to be the data hub of the GBA (and beyond), a step further by adopting the mandatory appointment of a DPO within an organisation is considered a key element, as it reflects good data governance.

[96] PCPD, Cross Border/Boundary Data Transfer in Hong Kong (March 2019), https://www.pcpd.org.hk/english/news_events/speech/files/CrossBorderBoundaryDataTransferb.pdf (accessed on 6 March 2022)

[97] Please refer to "Hong Kong" from the section of "Common mechanisms for cross-border data transfer for additional information.

[98] European Commission, "What are the responsibilities of a Data Protection Officer (DPO)?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en (accessed on 31 August 2022)

[99] PCPD, Privacy Management Programme: A Best Practice Guide (August 2018), https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf; PCPD, Privacy Management Programme (PMP) Manual; https://www.pcpd.org.hk/misc/files/grg_private_sector.pdf (both were accessed on 24 October 2022)

To strengthen data governance and policy coordination within the GBA

Recognising the complexity of harmonising data regulations for cross-boundary transfer between Hong Kong and GBA cities in Mainland China, it is suggested that the Hong Kong Government should maintain a dialogue with its Mainland counterparts to enhance governance and policy coordination among relevant authorities within the GBA.

Notably, Mainland China has signed two data security frameworks, namely the China-League of Arab States (LAS) Cooperation Initiative on Data Security (China-LAS DSCI) in March 2021,[100] and the Data Security Cooperation Initiative of China + Central Asia (C+C5 DSCI) in June 2022,[101] with a view to strengthening data cooperation and promoting digital economy among the signing member countries. While these initiatives are not directly related to cross-border/boundary data sharing, it is clear that stronger cooperation in data-related matters are crucial for the digital economy. Hong Kong, being part of China, should aim to develop stronger cooperation with the Mainland in data related initiatives, particularly governance related to data connectivity.

Having a mutual understanding of the rules and regulations in each other's jurisdictions can be fostered through rolling out various forms of pilot projects as the process would allow fast tracking cross-boundary data exchanges for certain data types among some GBA cities, subject to certain rules and protocols that are agreeable to the relevant parties involved. In the long run, these initiatives can be scaled to the wider GBA area, based on regulatory and enforcement experience accumulated. As such, a more harmonised data governance standard that is applicable to the entire GBA can be developed, to enable more secure and efficient data flow.

It is equally important to strengthen policy coordination within the GBA, for the purpose of enabling data sharing and usage across boundaries. Hence, the Hong Kong Government should consider setting up a joint advisory group/committee with its counterparts and, if appropriate, invite other relevant public sector stakeholders of Mainland China, such as the Cyberspace Administration of China and financial supervisory bodies, to provide support and resources. Support from the Central Government would certainly help to accelerate the implementation progress.

[100] People's Republic of China, Ministry of Foreign Affairs, "China-League of Arab States Cooperation Initiative on Data Security" (29 March 2021), https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202103/t20210329_9170559.html (accessed on 15 July 2022)

[101] People's Republic of China, Ministry of Foreign Affairs, "Wang Yi Attends the Third "China+Central Asia" Foreign Ministers' Meeting" (9 June 2022), https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202206/t20220609_10700621.html (accessed on 15 July 2022)

To establish white- and grey-lists to facilitate cross-boundary data transfers within the GBA

Under the current legal setup, data leaving Mainland China and Hong Kong are subject to various degrees of regulatory approvals and obligations. It is therefore suggested that the Hong Kong Government and its Mainland counterparts relax or exempt the regulatory requirements of certain types of data to promote the financial services industry within the GBA, subject to rules and protocols with defined accountability for the safety and security of data being transferred. Such an approach can be represented in the form of a white-list and grey-list. A white-list will permit certain categories of data to enter and exit freely; the grey-list is for the categories of data that are allowed to be transferred only within the GBA and no further transactions beyond the region.

The parameters for the data categories can be of specific industries (e.g., data from the financial services industry for the purposes of cross-boundary remittance and payment), specific company sizes (e.g., SMEs), specific purposes (e.g., regulatory compliance, anti-money laundering/combating terrorist financing, or non-commercial research), and the parameters should be reviewed regularly and have the flexibility for adjustment as needed. In particular, the white-list should be comprehensive and as inclusive as practicable to enable a variety of data to be included as appropriate, which will maximise the range of businesses, customers, and financial activities who can benefit from such an arrangement.

We recognise that it is challenging to identify which data types should be included in each list, because the definition and scope of each type of data must be clearly and precisely defined. Therefore, when deciding the types of data to go under the white-list and grey-list, Hong Kong and relevant Mainland counterparts may draw references from other jurisdictions in terms of the approach to govern the transfer of certain data types. For example, for the white-list category, the Government could explore the feasibility of allowing banks to report and transfer relevant cross-boundary data that is critical to the internal management and risk control of businesses (e.g., suspicious trading transactions, network analysis). As for the grey-list, the Government and its Mainland counterparts could consider allowing the free flow of financial data related to various Connect Schemes, such as the Cross-boundary Wealth Management Connect Scheme, within the GBA, but still prohibit further transfers outside of the region. Freer flow of such information will help foster the enhancement and growth of various Connect Schemes.

As previously mentioned, section 33 of the PDPO (although not in effect) currently operates a "whitelist", which is tied with the data laws of the receiving jurisdictions (i.e., the transfer of data is permitted if a receiving jurisdiction has a privacy law similar to the PDPO). The suggested white- and grey-lists will be tied to the categories of data, which would hopefully provide businesses with more flexibility for data transfer and will allow for freer data transfer than a simple jurisdictional white-list (i.e., a simple yes/no situation). However, we also recognise that having an extra two lists might create additional compliance challenges for businesses as they will need to categorise their data, which can be difficult. Nonetheless, we believe this recommendation will be effective in facilitating cross-boundary data transfers, and the additional compliance challenges can possibly be overcome by having well-defined definitions for the two lists, as well as by adopting a two-phased approach to implement, namely to start with introducing a white-list, then roll out a grey-list after businesses are familiar with such processes.

To explore the feasibility of cross-boundary data sharing through conducting pilot projects

Apart from the recommendation to set up white- and grey-lists, other pilot projects can be explored by imposing less restrictive requirements for an easier flow of financial-related data among specific financial institutions and companies. In the initial stage, these pilot projects can be limited to data flow within selected GBA cities, to ensure the programmes are implemented in a gradual and risk-manageable manner.

The Government can, for example, take reference of the policies of Free Trade Zones, such as Hainan,[102] Shanghai,[103] Beijing,[104] among others to conduct pilot projects for cross-boundary provision of data related to the financial services industry within the GBA. In this context, the process of security assessment, certification, and standard contract review process can be simplified. The scope of data can also include, or gradually add in, data that is less sensitive, SME related, business operations, and non-commercial research metrics. The white- and grey-lists mentioned previously can be considered as one of the approaches to implement such pilot projects.

Many policies are already in place to actively promote the connections between the financial services industry in the GBA, including the cross-boundary use of Renminbi, investment and wealth management, and insurance products. These polices have formed the foundation for cross-boundary financial data policies. Efforts should be made to explore how data sharing can be implemented within cross-boundary financial products and services.

For example, for the Wealth Management Connect, authorities should explore the possibility to allow investors in Hong Kong to open a cross-boundary northbound investment account without the need to be physically present at a Mainland branch (i.e., remote client on-boarding). Additionally, the Government should explore ways to enable more efficient data transfer between banks and sources of commercial data, to support SMEs and start-ups in the GBA to expand across the boundaries, fostering economic growth.

Another Free Trade Zone reference is the Shanghai Lin-Gang Special Area, which has proposed allowing eligible foreign financial institutions to report and transfer relevant data involving their holding of financial institutions in Mainland China abroad for group management purposes, especially those data that are crucial for the internal management and risk control of business operations.[105]

Launching pilot projects in experimental business zones or special economic zones within the GBA should be further explored. For example, the Qianhai Shenzhen-Hong Kong Modern Service Industry Cooperation Zone (Qianhai Cooperation Zone) has been set up as an experimental business zone to facilitate cooperation between Mainland China and Hong Kong in financial services, IT services and logistics activities. Thus, the Qianhai Cooperation Zone will be an ideal place for conducting pilot projects. Hong Kong may also consider leveraging Shenzhen's greater autonomy in policy setting as

---

[102] The People's Republic of China, 中共中央国务院印发海南自由贸易港建设总体方案 (1 June 2020), http://www.gov.cn/zhengce/2020-06/01/content_5516608.htm (accessed on15 February 2022)

[103] People's Government of Shanghai, 上海市人民政府关于印发《上海市全面深化服务贸易创新发展试点实施方案》的通知 (5 November 2020), https://www.cs.com.cn/xwzx/hg/202011/t20201113_6111251.html (accessed on 25 February 2022)

[104] The People's Government of Beijing Municipality, 北京市商务局关于印发《北京市关于打造数字贸易试验区实施方案》的通知 (18 September 2020), http://www.beijing.gov.cn/zhengce/zhengcefagui/202009/t20200923_2088196.html (accessed on 16 June 2022)

[105] People's Government of Shanghai, 上海市人民政府关于印发《上海市全面深化服务贸易创新发展试点实施方案》的通知 (5 November 2020), https://www.cs.com.cn/xwzx/hg/202011/t20201113_6111251.html (accessed on 25 February 2022)

a “Special Economic Zone”, or concessionary policies rolled out for the Qianhai Cooperation Zone, to explore different options with a view of facilitating data flow between Shenzhen and Hong Kong.

It is also suggested that a “data customs” could be established within the GBA with an aim of regulating cross-boundary data transfer and supporting the integration of data for the region. The FSDC recommends finding common denominators of the existing data laws between Mainland China and Hong Kong to formulate a set of rules, regulations, and guidelines for different purposes/circumstances of cross-boundary data transfer; a risk-based data flow model can also be explored. It is believed that an effective integration of different regulatory frameworks and basic systems will strengthen mutual trust in cross-boundary data cooperation and eventually drive the enhancement of regulations across the GBA.

With an aim of taking forward the pilot projects, setting up a task force joined by industry representatives is recommended to steer and facilitate the overall coordination. Some of the key factors the task force may wish to address are the duration, scale, locations, implementation, monitoring and evaluation of pilot projects as well as the timeline and roadmap to extend pilot projects to the wider GBA region.

To develop a set of GBA data governance standards

In the long run, Hong Kong should aim to collaborate with Mainland China to develop a ‘GBA-wide’ legal and regulatory data framework that reduces friction for transferring data across the three jurisdictions. Standardised data governance will significantly reduce compliance cost for businesses and allow data to flow freely across industries and boundaries, thereby leading to greater connectivity, efficiency, and productivity within the region. The Government could consider drawing reference from the ASEAN Data Management Framework (DMF).[106] The DMF is a step-by-step guide for businesses to set up a data management system, including data governance structures and safeguards. A good data management system helps business to unlock the value of data while ensuring adequate safeguards. In fact, the Guangdong Government recognises the need to support data flow within the GBA effectively in order to accelerate the digital transformation of the GBA.[107] This is indicated by the Action Plan for the Reform of Market-based Allocation of Data Matters in Guangdong (the Action Plan), published by the Guangdong Government in July 2021. The Action Plan aims to promote the orderly flow of data within the GBA.[108] Specifically, it mentions that a common data centre for the GBA will be established to facilitate the orderly circulation and sharing of data among East, West, and North Guangdong and the GBA. In this context, several data application case studies can be formed to benefit industry development, social governance, and services for the people and related areas.

Leveraging these policy supports and the “One Country, Two Systems” principle, Hong Kong should establish a favourable legal and regulatory environment where market participants can tap into the business potentials of cross-boundary data transfer. Hong Kong should engage with relevant counterparts of Mainland China in building a consensus for compliance requirements for exporting data from Mainland China to Hong Kong, such as the security assessment, to fully contemplate the viability, demand, and features of the financial services industry.

---

[106] Personal Data Protection Commission of Singapore, ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows (January 2021), https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows (accessed on 4 March 2022)

[107] The People’s Government of Guangdong Province, 广东省人民政府关于印发广东省数据要素市场化配置改革行动方案的通知 (5 July 2021), http://www.gd.gov.cn/xxts/content/post_3342648.html (5 May 2022)

[108] The People’s Government of Guangdong Province, 广东省人民政府关于印发广东省数据要素市场化配置改革行动方案的通知 (5 July 2021), http://www.gd.gov.cn/xxts/content/post_3342648.html (5 May 2022)

Relatedly, it is important for Hong Kong to work closely with relevant Mainland authorities to provide a high degree of certainty to businesses,[109] including data processors that handle personal information of over one million users. Most ideally, the provision of personal information or data to Hong Kong and Macao for purposes of providing and receiving financial services should be granted the same level of convenience as onshore regions (境內) with reference to the "Data Security Law", "Personal Information Protection Law", and "Cyber Security Law" of Mainland China, among others. Notably, Hong Kong was selected as the location for the US Public Company Accounting Oversight Board (PCAOB) to conduct auditing on the finances of a number of US-listed Chinese companies in August 2022; such an arrangement is an example of how financial-related data can be transferred across boundaries.[110]

If cross-boundary personal information or data is required to be provided to countries or regions other than Hong Kong or Macao, security assessments, certifications, standard contract clauses, or other ring-fencing measures can be put in place in accordance with the requirements of cross-boundary data provision in the jurisdiction of Mainland China to prevent further transfer to overseas destinations to ensure the security and protection of onshore data. In this context, the enactment of section 33 of PDPO that governs cross-border/boundary data transfers is crucial.

Data governance framework with consideration of data ethics

Data protection and ethical data usage are highly relevant; hence, data ethics should be considered while formulating a standardised data governance framework within the GBA, with a view to minimising potential ethical risks and advocating the ethical use of data. Data ethics encompasses a sound knowledge of data protection law, moral obligations of handling personal identifiable information, and the appropriate use of new technologies.[111,112]. An ethical practice effectively promotes the responsible and sustainable use of data to benefit society, and ensures that knowledge obtained through data is not being exploited or causing harm to an individual or society.[113] Encouragingly, many jurisdictions and regional organisations have published good practices/principles and data ethics frameworks to guide the ethical use of data.

Furthermore, AI technology plays a key role in supporting the development and enhancement of the financial services industry, and integration within the GBA, as mentioned previously. In view of the increasing adoption, AI perhaps has a more significant impact on individuals and society, thus promoting AI governance is deemed necessary by industry practitioners. Notably, AI governance encompasses many aspects, with responsible AI increasingly becoming a key block of a comprehensive AI governance framework. Responsible AI is a set of principles with ethical and moral concerns considered,[114] with a view of fostering a positive impact on the development through guiding them to innovate responsibly and to cultivate a responsible culture.[115]

---

109 As mentioned before, these include data processors transferring important data abroad, operators of critical information infrastructure, data processors handling the personal information of over 1 million users, and data processors who have either accumulatively provided the personal information of over 100,000 users or sensitive information of over 10,000 users abroad since January 2021.

110 The New York Times, " U.S. and China Announce Deal to Share Audits of U.S.-Listed Chinese Firms" (26 August 2022), https://www.nytimes.com/2022/08/26/business/us-china-audit-deal.html (accessed 11 November 2022)

111 The Government of the UK, Data Ethics Framework: glossary and methodology (16 September 2020), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology (accessed on 2 September 2022)

112 Harvard Business School, 5 Principles of Data Ethics for Business (16 March 2021), https://online.hbs.edu/blog/post/data-ethics (accessed on 2 September 2022)

113 The Government of the UK, Data Ethics Framework: glossary and methodology (16 September 2020), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology (accessed on 2 September 2022)

114 International Technology Law Association, "Responsible AI: Policy Framework" (23 May 2019) https://www.itechlaw.org/sites/default/files/ResponsibleAI_PolicyFramework.pdf (accessed on 16 September 2022)

115 Microsoft, Responsible AI, https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6 (accessed on 16 September)

Many leading technology firms involve the use of data and AI concurrently, and hence they build data governance frameworks with principles that promote responsible AI. With that in mind, a common data ethics framework, including AI governance, should be incorporated into the 'GBA-wide' data governance. A common data ethics framework can take reference from Mainland China's "Guide to the Building of a National Standard Framework for New Generation Artificial Intelligence"[116] and the "Next Generation AI Ethical Regulations,[117] Hong Kong's Data Ethics for Small and Medium Enterprises[118] and Guidance on the Ethical Development and Use of Artificial Intelligence,[119] the UK's Data Ethics Framework[120], and OECD's Good Practice Principles for Data Ethics in the Public Sector,[121] while a common AI governance framework can take reference of the Ethical AI framework issued by Office of the Government Chief Information Officer (OGCIO), Mainland China's regulatory standards, as well as the international standards.

[116] People's Republic of China,《国家新一代人工智能标准体系建设指南》(7 July 2020), http://www.gov.cn/zhengce/zhengceku/2020-08/09/content_5533454.htm (accessed on 3 February 2022)

[117] Ministry of Science and Technology of the People's Republic of China,《新一代人工智能伦理规范》(26 September 2021), http://www.most.gov.cn/kjbgz/202109/t20210926_177063.html (accessed on 3 February 2022)

[118] PCPD, Data Ethics for Small and Medium Enterprises (April 2019), https://www.pcpd.org.hk/english/resources_centre/publications/files/dataethics_en.pdf (accessed on 2 September 2022)

[119] PCPD, Guidance on the Ethical Development and Use of Artificial Intelligence (August 2021), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf (accessed on 24 October 2022)

[120] The Government of the UK, Data Ethics Framework (16 September 2020), https://www.gov.uk/government/publications/data-ethics-framework (accessed on 2 September 2022)

[121] OECD, Good Practice Principles for Data Ethics in the Public Sector https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm (accessed on 2 September 2022)

To formulate standard contractual clauses for cross-boundary data transfers within the GBA

The GBA covers three jurisdictions, each with different legal systems. While this is the unique set up of the region, regulatory fragmentation should not become the impediment for integrating financial services industries within the region. The Government should actively work with relevant counterparts in Mainland China (and Macao) to formulate a set of standard contractual clauses that meet the regulatory requirements of the jurisdictions for businesses to overcome the challenges of complying with various data regulations across the region.

In order to achieve this, the Government could build on the SCCs issued by Mainland China and the PCPD's RMCs, which can be served as a starting point for formulating a set of GBA contractual clauses to facilitate cross-boundary data transfer. The Government could also consider drawing reference from the ASEAN's Model Contractual Clause for Cross Border Data Flows (MCCs) to formulate such model contractual clauses. The ASEAN MCCs is a key resource to support companies operating in ASEAN in data-related business operations.[122]

The MCCs, similar to the SCCs of Mainland China and the RMCs, are template contractual terms and conditions that can be incorporated in the legal binding agreements between companies when transferring personal data to each other across borders.[123] The template clauses help reduce the negotiation and compliance cost and time for businesses, while also ensuring the protection of personal data when it is transferred abroad. The introduction of similar practices will be helpful as a practical support for businesses to smooth compliance procedures that can help address some of the concerns over the implementation of section 33, as previously discussed.

[122] Personal Data Protection Commission of Singapore, ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows (January 2021), https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows (accessed on 4 March 2022)

[123] Personal Data Protection Commission of Singapore, ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows (January 2021), https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows (accessed on 4 March 2022)

To set up a third-party certification agency to conduct impartial conformity assessment on cross-boundary data transfers within the GBA

Many jurisdictions, including Mainland China and the EU, allow international data transfer if data users have obtained certain certifications issued by professional organisations that are recognised by local authorities or regulators. The Government should consider establishing an independent and professional organisation, or leveraging existing professional organisations if practical, to provide certifications to companies with robust data governance frameworks as trusted data users or processors for cross-boundary transfer within the GBA (and beyond in the future).

The organisation should be entrusted to issue certifications by making reference to a set of data governance principles, covering data security principles for the protection of the data being retained or analysed. A set of reliable data governance frameworks can be derived by referencing standards of other major jurisdictions, for instance, the DSL, PIPL, CSL, PDPO, and GDPR, as well as the GBA data governance standards and frameworks proposed in this research paper. Ideally the organisation should also have the capacity to issue certifications related to AI adoption, based on a set of AI standards indicated in the OGCIO Ethical AI framework. Similarly, references can be taken from the data regulations mentioned above.

For an organisation to be qualified as a certification agency, one should have sufficient expertise and experience of legal knowledge within the systems of Mainland China and Hong Kong, and should also be recognised by regulators of both sides. Hence, existing professional organisations that fulfil the criteria might be qualified to take up the role. Furthermore, the organisation should have the capacity to handle various types of certifications. An alternative solution is to set up professional bodies respectively in Mainland China and Hong Kong, with an endorsement from their corresponding authorities and mutual recognition from authorities of the other side. This could potentially be extended to other jurisdictions, such as the EU.

By benchmarking and certifying practices of data flow and AI against the data governance and AI framework mentioned above, it will demonstrate compliance with Hong Kong, Mainland China, and relevant overseas regulations, and demonstrate to the public the trustworthiness of data protection and AI practices. Hong Kong's reputation for professional services (including independent certification and cyber security) uniquely qualifies it to roll out such a certification framework to facilitate data exchange across the GBA and position Hong Kong as a trusted data hub for the GBA. In the long run, the scope of service of such a professional organisation could be expanded to cover other jurisdictions, including other Asian economies and potentially global jurisdictions, establishing Hong Kong as the genuine data hub of Asia and beyond.

To explore the use of new technologies to enable cross-boundary data transfers within the GBA

Apart from examining policy restrictions hindering smoother cross-boundary data exchanges, the Government should also explore the usage of innovative technologies to facilitate more efficient cross-boundary data sharing.

With proliferating international regulations on cross-border/boundary data exchange and rising concerns over data privacy from data subjects and regulators, new technologies are sought after for safe and efficient handling, storing, and processing data. One increasingly popular option is to adopt federated data analytics, which uses new technologies, such as cloud computing, domestically based data centres and blockchain to allow data to be stored locally and securely, while at the same time enabling users to perform analytics and generate insights to make business decisions.[124]

Various technological integrations have been adopted in data-oriented initiatives in different parts of the world, including the three examples listed below, which can provide reference for the Government.

Shenzhen and Singapore's Blockchain-based Transnational Trade Network (BTTN)

Closer to home, Shenzhen and Singapore, which are among the world's leading trading ports, have developed a blockchain-based data-exchange network to share trade information between the two locations. The initiative demonstrates their joint efforts to become smart cities for digital economic development by further enhancing data sharing in the field of trade.

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking both tangible and intangible assets.[125] Advantages of blockchain technology include greater trust, higher level of security, lower fees to intermediaries, faster transactions, easier tracking, account reconciliation automation, etc.[126]

According to a service provider of the BTTN project, its network is made up of data centres that are set up with BTTN software on a cloud server. Data centres are connected via blockchain-based data highways, known as business chains. Firms can exchange data across borders/boundaries by plugging into the data centres and access through business chains while in compliance with local regulations. The BTTN has built-in Systems-level Services that allows secure document transfer, decentralised identity verification, and decentralised data storage to support cross-border/boundary data sharing.[127]

The BTTN helps firms remain in compliance with local data privacy and security laws, as it claims to have "a strong governance system that complies with local and international laws". Regulators will also be able to assess whether a firm is compliant with their respective data regulations. Other advantages of using the BTTN include higher efficiency, security, and easiness for cross-border/boundary data sharing because the trade industry, such as the financial services industry, handles a large amount of data and is highly dependent on digitalisation and automation.

---

[124] SSRN, Financial Data Governance: The Datafication of Finance, the Rise of Open Banking and the End of the Data Centralization Paradigm by Douglas W. Arner, et al (23 March 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4040604 (accessed on 4 April 2022)

[125] An asset can be tangible (such as land, a vehicle, or cash) or intangible (such as intellectual property, copyrights, or branding).

[126] According to documents provided by a service provider of BTTN, Red Date Technology.

[127] According to documents provided by Red Date Technology.

According to media reports, Southern Electronic Ports, a branch of Mainland China's electronic port system, will set up a data centre in Shenzhen, and an investment fund company will set one up in Singapore, which will integrate with the IMDA-operated TradeTrust system.[128] Other participants including the China Centre for Urban Development, a branch of the National Development and Reform Commission (NDRC), Government Technology Agency of Singapore (GovTech Singapore) and Tencent-backed neobank WeBank, and logistics supplier LinkLogis from the private sector.

Europe's Gaia-X Infrastructure

In light of the numerous data initiatives and frameworks within the EU that support better data governance and encourage non-personal data sharing between organisations, such as the European Data Strategy[129] and the European Data Act,[130] the public and private sectors of Europe are exploring alternative solutions to facilitate data sharing within Europe to promote better use of data and drive growth. The European Data Strategy "aims to make the EU a leader in a data-driven society" by "creating a single market for data [that] allow [data] to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations."[131]

Motivated by the abovementioned aspirations, European businesses and organisations from various sectors have developed, albeit still a work-in-progress,[132], a Gaia-X infrastructure, which uses innovative technology to build an infrastructure that facilitates free and secure flow of data within the region. The Gaia-X project was initiated by Germany and France with an aim of building a federated and secure data ecosystem based on European standards that align with the European Data Strategy.

All participants of the ecosystem must adhere to the high compliance thresholds that concern data security and protection. The ecosystem contains four main stakeholders, namely service providers, data providers, data owners, and data consumers. The data owners can "attach specific usage control policies to restrict access and use". Therefore, the ecosystem provides companies and citizens with a trusted environment to exchange data, while data owners can retain control over their data on the other end.

The infrastructure relies on technology such as cloud services, AI, Internet of Things applications, and analytics services. It is well supported by representatives from fields of business, politics, academics, and science from Europe and around the globe.[133] As of 26 March 2022, Gaia-X has over 1,800 contributors and 500 organisations, with 40% being SMEs, covering a range of industries such as mobility, energy, manufacturing, finance, agriculture, aerospace, public services, and healthcare.[134] Gaia-X infrastructure can facilitate effective data sharing between public and private institutions/organisations, between companies, and between industries, leading to more innovation.

---

[128] Yahoo, BSN's Red Date Behind Shenzhen-Singapore Trade Blockchain Project (19 January 2022),
[129] https://finance.yahoo.com/news/bsn-red-date-behind-shenzhen-163907281.html (accessed on 3 April 2022)
European Commission, The European Data Strategy (19 February 2020), https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283 (accessed on 4 April 2022)
[130] European Commission, Data Act (16 March 2022), https://digital-strategy.ec.europa.eu/en/policies/data-act (accessed on 4 April 2022)
[131] European Commission, The European Data Strategy (19 February 2020), https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283 (accessed on 4 April 2022)
[132] For example, the GAIA-X infrastructure has been criticised for repeatedly missing deadlines due to too many disagreements between stakeholders. Please see https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/
[133] Gaix-X, https://www.gaia-x.eu/what-gaia-x/factsheet (accessed on 4 April 2022)
[134] Gaix-X, https://www.gaia-x.eu/what-gaia-x/factsheet (accessed on 4 April 2022)

User-held data model and self-sovereign identity

Privacy regulations such as the GDPR in Europe have, as mentioned before, increased compliance costs for businesses given the additional resources required to ensure their internal data management processes are aligned with newly imposed regulatory requirements, as well as to provide relevant staff training. That said, the emergence of innovation for the storage, processing, and handling of personal data prompted by the growing concerns and regulations around data handling is observed. In particular, the rising trend of the user-held data model, can effectively facilitate companies to reduce compliance risks.[135]

Under the user-held data model, where "individuals maintain digital copies of their raw personal data in one place (a personal data cloud)",[136] users have full ownership and control over their own personal data, including how data is used, which companies will be granted access, and the level of data to be shared. Access to the personal data cloud is restricted to individual data owners. Prior authorisation should be sought from them prior to the access.

Third parties who wish to access the information require authorisation from data owners in advance and only fragmented/selected info will be available. Such an arrangement effectively helps data owners to retain control over their personal data, while mitigating compliance risks for businesses.

Another user-centric approach to address concerns around privacy issues is self-sovereign identity. While there is no agreed definition on self-sovereign identity, the "core notion is arguably that users are given control and autonomy over their identity data, how it is used and who it is used by."[137] Without getting into the technicality of self-sovereign identity, it is essentially built on an ecosystem, with blockchain technology being one of the three pillars.[138]

The personal information of users will be stored within an ecosystem, rather than on a central database, which is the traditional way of storing personal data online.[139] Users can then choose to reveal only the necessary information to an entity for a given interaction, hence increasing the security and privacy of the users. The application of such technology is promoted and has been adopted in many fields, including for building credit history and sharing COVID-19 information.[140]

We believe that the BTTN project and the Gaia-X Infrastructure can provide a useful reference for facilitating data exchange, whereas user centric approaches to store personal data can shed light on effective ways to address potential data privacy concerns. It is, therefore, recommended that the Government considers adopting these new technologies in order to create conducive conditions for the city to become a financial data hub of the GBA.

---

[135] Harvard Journal of Law and Technology, My Data, My Terms: A Proposal for Personal Data Use Licenses (5 March 2020), https://jolt.law.harvard.edu/digest/my-data-my-terms (accessed on 16 June 2022)

[136] Harvard Journal of Law and Technology, My Data, My Terms: A Proposal for Personal Data Use Licenses (5 March 2020), https://jolt.law.harvard.edu/digest/my-data-my-terms (accessed on 16 June 2022)

[137] World Economic Forum, Self-sovereign identity: the future of personal data ownership? (12 August 2021), https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/ (15 June 2022)

[138] The other two pillars are public-key cryptography and decentralized identifiers. Please refer to: World Economic Forum, Self-sovereign identity: the future of personal data ownership? (12 August 2021), https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/ (15 June 2022)

[139] World Economic Forum, Self-sovereign identity: the future of personal data ownership? (12 August 2021), https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/ (15 June 2022)

[140] World Economic Forum, Self-sovereign identity: the future of personal data ownership? (12 August 2021), https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/ (15 June 2022)

To attract and cultivate talent with technological and digital-related skillsets

In order to develop Hong Kong into a data hub of the GBA, growing relevant talent in the city is deemed crucial. The city should be well supported by talent with expertise in a broad range of areas, from data science, AI, digital innovation, to business acumen, and financial analytics, to name a few, to position itself as the data connector for the GBA. However, Hong Kong, like many markets, face challenges of talent shortage with technological and digital skills. Not only because talent is in short supply, but also the surging demand for such talent due to digitalisation of the financial industry and other professional industries. Against this backdrop, it is suggested that the Government, industry players, and universities should actively seek to address this issue and enhance collaboration between the three.

To adjust visa application process for foreign specialists

While pandemic control measures are necessary to protect Hong Kong from the looming threat of COVID-19 variants, it may be beneficial to explore facilitative measures to expedite the approval process for critical sectors, especially the Technology Talent Admission Scheme (TechTAS). In 2021, the Scheme only approved 60 applications (out of 64 applications received), as compared to 116 applications approved (out of 131 applications received) in 2020,[141] pointing towards a significant decline in technology-related talent admitted via the scheme.

While the reason for this trend is unclear to track (e.g., reduction in applications, stricter screening procedures), the Government should consider fully utilising the scheme as a fast-track arrangement for specialised talent, including by further expanding the scope of eligibility,[142] or uplifting existing pre-allocated quota.

To attract talent from Mainland GBA cities

Apart from acquiring foreign specialists, Hong Kong should also attract talent from the GBA. The GBA offers Hong Kong a large talent pool that it can readily access. Notably, the region has a population of around 79 million[143] and is home to some of the most valuable unicorns in the world.[144] According to the Hurun Global Unicorn Index 2022 Half-Year Report, Mainland China was ranked second for the highest number of unicorns at 312, out of which Shenzhen has 33 and Guangzhou has 19 unicorns, compared to seven in Hong Kong.[145]

One key factor that will enhance our attractiveness to talent from other GBA cities is to improve talent mobility, i.e., the freer flow of people within the region. With better talent mobility, while talent from other GBA cities can contribute to Hong Kong's Fintech ecosystem, Hong Kong can also provide financial expertise to the region, leading to a two-way talent flow and deepening the integration of the region. In order to facilitate cross-boundary talent mobility, further study and adjustments will be needed regarding the current immigration regime.

---

141 HKSAR, "Applications for Visa/Entry Permit under the Technology Talent Admission Scheme" (4 May 2022), https://gia.info.gov.hk/general/202205/04/P2022050400281_392037_1_1651639421009.pdf (accessed on 27 June 2022)

142 The TechTAS scheme has a narrow eligibility criterion that focuses on research & development work, with a non-exhaustive exclusion list that the hiring company will have the onus of proof. In 2020, the scheme has been amended to add six new technology areas to the existing seven technology areas covered by the scheme

143 Hong Kong Trade Development Council, 粵港澳大灣區統計數字, https://research.hktdc.com/tc/article/MzYzMDE5NzQ5 (accessed on 2 September 2022)

144 Hurun, 2022年中全球獨角獸榜 (30 August 2022), https://www.hurun.net/zh-CN/Info/Detail?num=L9SQPH9FKJB1 (accessed on 2 September 2022)

145 Hurun, 2022年中全球獨角獸榜 (30 August 2022), https://www.hurun.net/zh-CN/Info/Detail?num=L9SQPH9FKJB1 (accessed on 2 September 2022)

To explore closer collaboration between Hong Kong universities and industry players

In recent years, there is evidence that Hong Kong universities are moving fast to tailor their courses and prepare their students to adapt to the actual working environment. For example, the University of Hong Kong (HKU) launched five new undergraduate programmes to nurture big data talent in October 2021.[146] Notably, HKU offers the only undergraduate Bioinformatics degree in Hong Kong to nurture future professionals in the biomedical data science field. Aside from undergraduate programmes, Hong Kong universities have also tailored their MBA courses to meet the cultural and technological needs of the GBA. The Hong Kong Polytechnic University has recently remodelled its MBA programme to keep pace with the latest developments, including new technological elements such as AI, blockchain, cloud computing, and data science in their curriculum.[147]

To take these encouraging developments to a new level, Hong Kong universities should consider working with industry players to develop practical content and training opportunities in the real business environment. Such practical experience can effectively train students' critical thinking and problem-solving abilities, in addition to theories learnt in classroom setting.

Notably, the HKMA has launched different fintech talent development programmes, some of which are collaborations with universities. These programmes target young talent, including university students, young graduates, and professionals, with a view to equipping them with practical knowledge to strengthen the talent pool. Universities can ride on such partnerships and expand to other industry players.[148]

Collective and coordinated efforts between the Government and industry players

While the Government has been introducing many talent development initiatives to support the industry's needs, there is room to harmonise these different programmes into a single go-to platform. For example, the Government's Reindustrialisation and Technology Training Programmes subsidises advanced tech training for employees of local companies, and has benefited more than 2,000 workers with funding of more than HK$13 million. This, coupled with the many different talent programmes offered by various government agencies (e.g., the Banking Talent Program), may duplicate resources in their operations. One way to achieve this is to consider streamlining/consolidating all public technology talent-related initiatives and ensure that there is minimal overlap between the different schemes; for example, the target graduates' segment. This might also achieve greater synergy as the Government could maintain a single repository of graduates who have been recruited by any of its talent schemes and ensure an efficient tracking mechanism.

[146] The University of Hong Kong, HKU launches new undergraduate programmes to nurture big data talents (27 October 2021), https://www.hku.hk/press/news_detail_23459.html (accessed on 18 January 2022)
[147] SCMP, Hong Kong's universities retool their MBA courses to meet the cultural and technological needs of the times and of the Greater Bay Area economy (10 January 2022), https://www.scmp.com/special-reports/article/3160939/hong-kongs-universities-retool-their-mba-courses-meet-cultural-and (accessed on 18 January 2022)
[148] HKMA, Fintech Talent Development (8 July 2022), https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/talent-development/ (accessed on 24 October 2022)

The above proposed recommendations are some of the potential solutions to create the supply of relevant talent to position Hong Kong as the data hub for the GBA. Cultivating a talent ecosystem to grow, retain, and attract relevant experts with technological or digital related skillsets requires concerted efforts between the private and public sectors, thereby creating a more sustainable talent pool. This is not only critical to facilitate Hong Kong in becoming a data hub for the region, but will also help to advance the digitalisation of Hong Kong.

The FSDC is encouraged by the Government introducing a series of new initiatives to nurture and attract talent, as laid out by the Chief Executive in his first Policy Address.[149] Initiatives such as the launch of the Top Talent Pass Scheme and relaxation of the stamp duty scheme will help to further strengthen the talent pool by attracting global talent. The FSDC is committed to working with relevant industries and the Government to attract talent, and has published a research paper titled "Careers of Tomorrow: Financial Talents in the Digital, Sustainable Economy of Hong Kong" in 2021 with recommendations to facilitate the cultivation of Hong Kong's financial talent for a digital and sustained economy.[150]

[149] HKSAR, Policy Address (October 2022), https://www.policyaddress.gov.hk/2022/en/policy.html（accessed on 28 October 2022)

[150] FSDC Research Paper No. 50, August 2021, https://www.fsdc.org.hk/en/insights/careers-of-tomorrow-financial-talents-in-the-digital-sustainable-economy-of-hong-kong

Conclusion

The free flow of financial data is important for the GBA region to unlock further growth potential alongside the future integration. The current legal set up among GBA cities makes data sharing between Hong Kong and other GBA cities unintentionally challenging, hence undermining the efficiency for businesses operating in the region. In this context, a financial data hub to facilitate the free flow of data is needed. Hong Kong, as an international financial centre with a world-class IT infrastructure, has a strong foundation to become the financial data hub to enable smoother data exchange within the region. This is in line with global trends as well, as many regional economic zones have also developed various mechanisms and approaches to facilitate the easier flow of data among their economies. Hence, Hong Kong (and the GBA) should keep up with the pace.

With the aim of developing Hong Kong into a financial data hub, the Government should provide clarity to its data polices and laws, particularly section 33 of the PDPO and laws related to cyber security. Furthermore, the Government should work with its mainland counterparts to develop a cross-boundary data governance standard, which can first start with implementing pilot projects; adopting innovative technologies to help overcome some compliance challenges/legal challenges derived from various data laws among the three legal systems within the GBA; and cultivating relevant talent.

The FSDC recognises that developing Hong Kong into a regional financial data hub requires concerted efforts, support and coordination from all pertinent actors, as well as more in-depth study in other complementary areas that may not have been covered in this research report. For instance, enhancing current data hub-related infrastructures (such as data centres), and reviewing current rules and guidelines (such as data-related guidelines published by the OGCIO[151] and laws related to cyber security) to ensure their relevancy. In this context, the FSDC believes that the recommendations set forth in this paper could provide guidance as an essential first step towards positioning Hong Kong as the financial data hub of the GBA, and preparing the city to be the regional financial data hub for Asia and beyond. Therefore, further enhancing Hong Kong's position as an international financial centre.

[151] OGCIO, Green Data Centres Practice Guide, https://www.ogcio.gov.hk/en/our_work/business/tech_promotion/green_computing/green_data_centre.html (accessed on 2 September 2022)

Appendices

Appendix 1. Key data regulation developments in Mainland China over the last five years

Table 1. (As of July 2022)

Effective Date / Issued Date	Leading Authority	Rule	Source
1 Jun 2017	Cyberspace Administration of China (CAC)	Cyber Security Law 《網絡安全法》	http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm
17 Aug 2021	State Administration for Market Regulation (SAMR)	Prohibition of Unfair Internet Competition (Draft) 《禁止網絡不正當競爭行為規定 (公開徵求意見稿) 》	https://www.samr.gov.cn/hd/zjdc/202108/t20210817_333683.html
1 Sep 2021	CAC and public security and state security organs	Data Security Law 《數據安全法》	http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml
1 Sep 2021	CAC, public security organs and Ministry of Industry and Information Technology (MIIT)	Security Protection of Critical Information Infrastructure 《關鍵信息基礎設施安全保護條例》	http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm
17 Sep 2021	CAC	Guiding Opinions on Strengthening the Comprehensive Management of Internet Information Service Algorithms 《關於加強互聯網信息服務算法綜合治理的指導意見》	http://www.cac.gov.cn/2021-09/29/c_1634507915623047.htm
1 Nov 2021	CAC	Personal Information Protection Law 《個人信息保護法》	http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
14 Nov 2021	CAC	Regulations on Network Data Security Management (Consultation Draft) 《網絡數據安全管理條例 (徵求意見稿) 》	http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm

Effective Date / Issued Date	Leading Authority	Rule	Source
30 Nov 2021	MIIT	14th FYP for Big Data Industry Development 《"十四五"大數據產業發展規劃》	http://www.gov.cn/zhengce/zhengceku/2021-11/30/5655089/files/d1db3abb2dff4c859ee49850b63b07e2.pdf
13 Jan 2022	National Information Standardization Technical Committee (TC260)	Information security technology – Rules for identification of key data (Draft)《信息安全技術重要數據識別規則(徵求意見稿)》 Formerly known as Information security technology: Guideline on Identifying Key Data (Draft)《信息安全技術重要數據識別指南(徵求意見稿)》)	http://std.samr.gov.cn/gb/search/gbDetailed?id=ACFF6A97D6EC2AB2E05397BE0A0A54AB ; http://tradeinservices.mofcom.gov.cn/article/szmy/zjyjgd/202204/133184.html
10 Feb 2022	MIIT	Measures for the Administration of Data Security in the Field of Industry and Information Technology (Draft) 《工業和信息化領域數據安全管理辦法(試行)》	https://www.miit.gov.cn/gzcy/yjzj/art/2022/art_d9a3a5efd4f64788b40c3af55d62e209.html
15 Feb 2022	CAC	Measures for Cyber Security Review 《網絡安全審查辦法》	http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm
30 Jun 2022	CAC	Chinese Standard Contractual Clauses for cross-border personal information transfer (Draft) 《個人信息出境標準合同規定（徵求意見稿）》	http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm

Effective Date / Issued Date	Leading Authority	Rule	Source
1 Aug 2022	SAMR	Anti-Monopoly Law (2022 Edition) 《反壟斷法(2022修正)》	http://www.gov.cn/xinwen/2022-06/25/content_5697697.htm
1 Aug 2022	CAC	Management of Internet User Account Information《互聯網用戶賬號名稱信息管理規定》	http://www.cac.gov.cn/2022-06/26/c_1657868775042841.htm
31 Aug 2022	CAC	Data Outbound Security Assessment Declaration Guidelines (First Edition) 《數據出境安全評估申報指南(第一版)》	http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm
1 Sep 2022	CAC	Data Outbound Security Assessment Measure 《數據出境安全評估辦法》	http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm

Appendix 2. A summary of data landscape and policies in Mainland China and Hong Kong

Table 2

	Mainland China	Hong Kong
Key Data Laws	• Cyber Security Law • Data Security Law • Personal Information Protection Law	• The Personal Data (Privacy) Ordinance (section 33 has not been implemented) • Hong Kong does not have specific cyber security legislation, but relevant provisions are found across various ordinances.[152]
Key data regulated	• Personal data • Important data collected and generated by operators of critical Information infrastructure	Personal data
Data localisation	Data localisation for Information from several specific sectors	No specific requirements
Cross-border/ boundary data transfer approval	Government Approval (Security Assessment) for operators of critical Information Infrastructure (CIIO) and personal information processors that process personal Information exceeding the volume threshold determined by the CAC	No specific requirements
Enabling guidelines and standards	• Obtaining certification on personal Information protection from an accredited certification body • Adopting the standard data transfer agreement with overseas recipient (Chinese Standard Contractual Clauses)	Adopting the standard data transfer agreement with overseas recipient (Recommended Model Contractual Clauses)
Key regulators	• Cyberspace Administration of China (CAC) • Ministry of Public Security • Ministry of Industry and Information Technology	The Office of the Privacy Commissioner for Personal Data (PCPD)

[152] Baker McKenzie, "Hong Kong: Updates to cybercrime and cybersecurity laws" (9 September 2022), https://insightplus.bakermckenzie.com/bm/data-technology/hong-kong-updates-to-cybercrime-and-cybersecurity-laws#cntAnchor5 (accessed on 24 November 2022)

Appendix 3. AI ethical standards and requirements in Mainland China and Hong Kong and other international standards

Mainland China AI Ethical Standards and Requirements

In Mainland China, the Standardization Administration published a framework for the development of AI related standards called "the Guide to the Building of a National Standard Framework for New Generation Artificial Intelligence"[153] on 5 August 2020. The guide explains that by 2023, a com prehensive framework of AI related standards for Mainland China will be established to encompass the development of data, algorithms, systems, services, and other key domains to support the adoption of AI technologies in manufacturing, transportation, finance, construction, and other key industries and fields.

The artificial intelligence standards framework is designed to address eight key areas, covering basic commonality, supporting technologies and products, basic software and hardware platforms, key general technologies, key field technologies, products and services, industry applications, and safety/ethics.

Other than the above guidelines, on 25 September 2021, the National New Generation Artificial Intelligence Governance Specialist Committee published the "Next Generation AI Ethical Regulations"[154] which is the first set of regulations published in this area. The purpose of the regulation is to incorporate ethics into the entire AI life cycle and to provide ethical guidance to natural persons, legal persons, and other related institutions engaged in AI-related activities. The regulation highlights the four Ethical Norms for New Generation Artificial Intelligence (Ethical Norms), which are:

- **Management Norms,** including promote agile governance, actively implement and demonstrate AI ethical governance, correctly exercise authority, strengthen risk prevention, and promote tolerance and openness;
- **R&D Norms,** including strengthen self-discipline consciousness, improve data quality, enhance security and transparency, and avoid bias and discrimination;
- **Supply Norms,** including respect market rules, strengthen quality control, safeguard user rights and interests, and strengthen emergency support; and
- **Use Norms,** including promote well-intentioned use, avoid misuse, prohibit violations and malicious use, actively provide prompt feedback, and improve use abilities.

These norms have been established in order to heighten society's ethical awareness and behavioural consciousness of AI, actively guide responsible AI R&D and application activities, and promote healthy AI development.

[153] People's Republic of China,《国家新一代人工智能标准体系建设指南》(7 July 2020), http://www.gov.cn/zhengce/zhengceku/2020-08/09/content_5533454.htm (accessed on 3 February 2022)

[154] Ministry of Science and Technology of the People's Republic of China,《新一代人工智能伦理规范》(26 September 2021), http://www.most.gov.cn/kjbgz/202109/t20210926_177063.html (accessed on 3 February 2022)

Hong Kong AI Ethical Standards and Requirements

In Hong Kong, both the HKMA and the PCPD have issued guidelines related to AI Ethical Standards and Requirements.

The growing use of AI presents not only opportunities, but also new risk management challenges to banks; therefore, the HKMA has issued guidelines called "High-level Principles on Artificial Intelligence"[155] on 1 November 2019 to provide guidance to the banking industry on the use of AI applications. The guideline consists of three principles related to governance, application design and development, and monitoring and maintenance. Additionally, the HKMA issued another guideline namely "Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence (BDAI) by Authorized Institutions[156]" on 5 November 2019. The guiding principles focus on four major areas, namely governance and accountability, fairness, transparency and disclosure, and data privacy and protection.

AI has huge potential to boost productivity and economic growth. As such, the rapid adoption of AI raises privacy and ethical concerns. In view of this, the PCPD issued the "Guidance on the Ethical Development and Use of Artificial Intelligence" ("Guidance")[157] on 18 August 2021 to help organisations understand and comply with the relevant requirements of the PDPO when they develop or use AI. In line with international standards, the Guidance sets out the seven ethical principles for AI which includes Accountability, Human Oversight, Transparency and Interpretability, Data Privacy, Fairness, Beneficial AI and Reliability, Robustness, and Security.

On top of these guidelines issued by the HKMA and the PCPD, OGCIO has published the Ethical AI Framework for government bureaux and departments ("B/Ds") to address ethical concerns and risks for AI adoption. The Ethical AI Framework establishes 12 AI principles, including transparency and interpretability; reliability, robustness, and security; fairness; diversity and inclusion; human oversight; lawfulness and compliance; data privacy; safety; accountability; beneficial AI; cooperation and openness; and sustainability and just transition.

International Standards

In May 2020, the International Organisation for Standardisation ("ISO") published a new standard ISO/IEC TR 24028:2020 "Artificial intelligence in information technology – An overview of trustworthiness in artificial intelligence", which discusses how to establish trust in AI systems through transparency, explainability, controllability, etc. The ISO standard discusses approaches for evaluating and achieving AI systems' availability, resiliency, reliability, accuracy, safety, security, and privacy.

---

[155] HKMA, High-level Principles on Artificial Intelligence (1 November 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf, (accessed on 3 February 2022)

[156] HKMA, Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions (5 November 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf (accessed on 3 February 2019)

[157] PCPD, Guidance on the Ethical Development and Use of Artificial Intelligence (August 2021), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf (accessed on 3 February 2019)

In November 2021, the Artificial Intelligence working group of the ISO (ISO/IEC JTC 1/SC 42) further published the ISO/IEC TR 24027 “Information Technology – Artificial Intelligence – Bias in AI Systems and AI aided decision making” standard. The relationship between equality and algorithmic bias is discussed in this standard. Additionally, it discusses the causes and types of bias within AI decision making, as well as the corresponding problem-solving measures.

ISO also published ISO/IEC TR 24029-1:2021 “Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview” and ISO/IEC TR 29119-11:2020 “Software and systems engineering – Software testing – Part 11: Guidelines on the testing of AI-based systems” to guide the testing process.

Acknowledgements

The FSDC would like to thank the following working group members for their valuable input:

Mr Leiming Chen

Dr Dorothy Chau

Mr George Chen

Mr Andre Da Roza

Mr Ryan Fung

Mr William Gee

Dr Hu Zhanghong

Mr Jia Jia

Ms Lareina Wang

Mr Danny Wong Chun Keung

Mr Wen Xiao

Mr Peter Yan

Ms Fanny Yuen

The FSDC would also like to thank Professor Douglas Arner and Mr Tim Bailey for their contributions to this Paper.

The operation of the FSDC is led by:

Dr King Au
Executive Director

This report was prepared by the FSDC Policy Research Team:

Dr Rocky Tung
Director, Head of Policy Research

Ms Wivinia Luk
Senior Manager, Policy Research

Ms Jessie Chen
Manager, Policy Research

Ms Erica Chung
Manager, Policy Research

Ms Joyce Lee
Manager, Policy Research

Mr Kendrew Leung
Manager, Policy Research

Mr Clement Ho
Assistant Manager, Policy Research

Ms Mickey Sze
Analyst, Policy Research

Report Weblink

Weblink to the pdf version of this report

FSDC Weblink

Financial Services Development Council

About the FSDC

The FSDC was established in 2013 by the Hong Kong Special Administrative Region Government as a high-level, cross-sectoral advisory body to engage the industry in formulating proposals to promote the further development of the financial services industry of Hong Kong and to map out the strategic direction for the development.

The FSDC has been incorporated as a company limited by guarantee with effect from September 2018 to allow it to better discharge its functions through research, market promotion and human capital development with more flexibility.

Contact us

Email: enquiry@fsdc.org.hk
Tel: (852) 2493 1313
Website: www.fsdc.org.hk