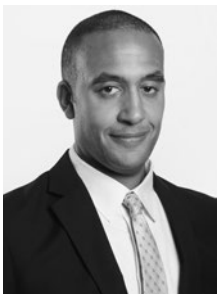
China's cross-border data sharing requirements: Compliance challenges for global institutions

Received (in revised form): 8th November, 2022

Eugenie Shen



Alex Roberts

Eugenie Shen*
Managing Director, Head of Asset Management Group, Asia Securities Industry & Financial Markets Association (ASIFMA), Hong Kong

Alex Roberts**
Counsel, Linklaters Shanghai Office, China

**Asia Securities Industry & Financial Markets Association (ASIFMA), Unit 3603, Tower 2, Lippo Centre, 89 Queensway, Admiralty, Hong Kong Tel: +852 2531 6570; E-mail: eshen@asifma.org*

***Linklaters Shanghai office, 29th Floor, Mirae Asset Tower, 166 Lu Jia Zui Ring Road, Shanghai 200120, China Tel: +86 21 2891 1842; Mob: +86 159 0900 6025; E-mail: alex.roberts@linklaters.com*

Journal of Financial Compliance
Vol. 6, No. 3 2023, pp. 198–212
© Henry Stewart Publications
2398-8053 (2023)

Eugenie Shen *is Managing Director and Head of ASIFMA's Asset Management Group (AAMG), which was set up as a separate division of ASIFMA in 2014 to represent asset managers in Asia, ex-Japan and ex-Australia. Like the rest of ASIFMA, AAMG focuses on the development of and access to capital markets in the Asia region. Eugenie is a US lawyer with decades of private practice and in-house legal experience across a wide range of institutions, industries and jurisdictions spanning Asia, the USA, Europe, and Latin America. Prior to joining ASIFMA, Eugenie was Regional Counsel of PineBridge Investments (the former AIG Investments) in Asia with responsibility for a number of asset management entities across the region. Her other former positions include Global General Counsel for the Sino-French joint venture television company TTE Corporation, Asia Counsel for private investment firm Morningside Technologies, Assistant Director and Head of China Listing at the Hong Kong Stock Exchange and Vice President and Senior Associate Counsel at Chase Manhattan Bank. Eugenie started her career as an associate at Shearman & Sterling, working in its New York and Hong Kong offices. She is a member of the New York Bar and has a BA from Cornell University and a JD from Georgetown University Law Centre.*

Alex Roberts *is Counsel at Linklaters' Shanghai office. He advises on a wide range of tech and data-related projects including cross-border tech acquisitions, investments into, and establishments of, online platforms, commercial contracts and operational compliance. With a growing web of data protection and cyber security regimes across the Asia region, Alex's work increasingly involves advising on regional data breaches, ransomware attacks and data compliance projects. He is currently advising numerous multinationals on implementation of mainland China's Personal Information Protection Law and Data Security Law. Alex frequently shares his insights on data protection, cyber security and broader TMT topics at leading media outlets such as Thomson Reuters, South China Morning Post, Global Data Review and Forbes. He is also a popular speaker at seminars and webinars on tech and data topics in China and Asia. Alex is qualified as a solicitor in England and Wales and holds a BA from Cambridge University. He attended the Legal Practice Course (English Law) at BPP Law School, London and holds a Graduate Diploma in Law from Nottingham Law School. Alex has also completed an executive MBA at China Europe International Business School in Shanghai, a course currently ranked fifth in the Financial Times rankings. Alex is also a member of the Executive Committee and is Advocacy Lead of the British Chamber of Commerce in Shanghai, acting as a channel for foreign business investigating entering and expanding in the mainland China market. Alex was recognised as a 'rising star' in the corporate and M&A, Fintech and TMT practices in China by Legal 500 in 2021 and 2022.*

Abstract

To protect public and societal interest, ensure network security and safeguard national security, China has passed a series of data security and data

protection laws in the past few years which, due to the cross-border data transfer or sharing restrictions under these laws, pose particular challenges for global institutions, especially financial institutions, which need information from their subsidiaries or counterparts in China. This paper summarises the three principal laws that govern the collection, storage, transfer and use of data within China and what global institutions with connections to China need to know.

Keywords: data security, data privacy, data transfer, personal information, Cyberspace Administration of China (CAC), China Securities and Regulatory Commission (CSRC)

INTRODUCTION

In 2021, the Data Security Law (DSL)[1] and the Personal Information Protection Law (PIPL)[2] in China came into force, together with a slew of data-related regulations or draft regulations that followed.

Together with the Cybersecurity Law (CSL),[3] which was passed in November 2016 with effect from 1st June, 2017, the DSL and PIPL form the over-arching regulatory framework for China's data security, protection and governance.

CHINA'S POLICY ON DATA

The stated purposes[4] of the CSL are to ensure the safety of the internet, safeguard national security, protect public interests and the lawful rights and interests of individuals and organisations, and promote the healthy development of economic and social informatisation. These objectives reflect China's policy in this area and the concepts embedded in the CSL are carried through to the DSL and PIPL and the other data-related laws and regulations.

China's recent data-related laws and regulations (such as the PIPL) are not unique and, like many other jurisdictions, are influenced by the General Data Protection Regulation (GDPR) adopted by the European Union (EU) on 14th April, 2016 and which became effective on 25th May, 2018. One of the primary aims of both the GDPR and the PIPL is to enhance protection of individuals' personal data. Nonetheless, unlike the focus on individuals' privacy rights under the GDPR, China's data laws (in particular, the DSL) are also tasked with, or more focused on, safeguarding national security and sovereignty and protecting public interests.

The GDPR provides flexibility for certain aspects of the regulation to be adjusted by individual EU member states, including where necessary for national security purposes. As an increasing number of countries develop or introduce their own data security laws and regulations, they are also linking data security to national security and sovereignty concerns. Navigating this convergence of policy and heightened regulation in the data security space has become a global issue.

CHINA'S DATA-RELATED LAWS

Set out below is a brief summary of the CSL, DSL and PIPL and some of the issues arising under these laws that global institutions should be aware of:

Cybersecurity Law

The CSL applies to the construction, operation, maintenance and usage of 'networks' and provides for network security supervision and management within China.[5]

What are networks and who are network operators?

Given that networks are defined quite broadly, referring to systems comprising computers or other information terminals and related equipment that follow certain rules and procedures for information

gathering, storage, transmission, exchange and processing,[6] almost all modern businesses would have or use networks. Network operators refer to network owners, managers and service providers, which again cover most individuals and entities.[7]

Obligation of network users

Individuals and organisations using networks have to abide by the laws, observe public order and respect social morality and not endanger network security or national security.[8]

Obligations of network operators

Network operators have to implement a network security protection system, which includes clarifying network responsibilities within their organisation, adopting measures to safeguard network operations, monitoring, recording and reporting network security incidents, as well as classifying data, and backing up and encrypting important data.[9] They also have to maintain confidentiality of user information that they collect[10] as well as to provide technical support and assistance to public security and national security authorities tasked with safeguarding national security and investigating criminal activities.[11]

The obligation to cooperate with public security and national security authorities echoes other existing laws, such as the Chinese National Intelligence Law and the Chinese National Security Law, which are vaguely drafted and could give a broad scope of interpretation to the Chinese authorities to apply to domestic organisations and individuals on a case-by-case basis.

As a result, for global institutions, especially financial institutions which have operations in the EU, where personal data needs to be transferred from the EU to China, a transfer impact assessment must be conducted to assess these Chinese laws applicable to data importers in the People's Republic of China (PRC). Issues such as the extent to which the personal data transferred might be accessed by the Chinese authorities and the safeguards necessary to protect the personal data transferred will need to be considered. Interestingly, the similarities between the EU's transfer impact assessment requirement and the security assessment requirement that applies to the export of data from China can be seen, as described below.

Obligations of crucial information infrastructure operators

Crucial network equipment and specialised network security products have to comply with national standards and requirements and be certified to meet safety requirements before they can be sold.[12] Crucial information infrastructure (CII) operators (CIIOs) each must set up a specialised security management unit, designate persons responsible for security management and conduct background checks on them, conduct periodic network security education and training, back up important systems and databases, conduct disaster recovery and organise drills etc.[13]

CIIOs that gather or produce personal information or 'important data' in China have to store such information within China[14] and undergo a national security assessment by the Cyberspace Administration of China (CAC) if they need to transfer such data outside China[15] or when they purchase network products and services that might affect national security.[16] CIIOs also have to sign a security and confidentiality agreement with the provider of network products and/or services to them.[17]

Compliance issues

A key issue for many companies is whether they are considered a network operator or a CIIO under the CSL, as the latter is subject to more onerous requirements.

The CSL introduced the concept of CIIO without providing an operationalisable definition, but this was clarified in the Regulations on Critical Information Infrastructure Security Protection[18] issued in July 2021. Under these implementation regulations, CII refers to important network facilities and information systems whose destruction or incapacity or data breach may have a debilitating impact on national security, national economy and the people's livelihood, and public interests.[19] Following this definition, operators in important industries and fields such as public communication and information services, energy, transportation, water resources, finance, public services, electronic government administration, and the national defence-related science and technology industry will be more likely to be identified as CIIO.[20]

These implementation regulations empower industry regulators to formulate further rules to identify CII and organise this identification within their respective industries and sectors.[21] A welcoming note under these regulations is that CIIOs will be informed of the results of this determination.[22] However, no supervising authorities have yet released a public list of CIIOs for their respective industries and sectors, an absence that creates legal uncertainty for organisations of a particular nature or scale.

Foreign companies with subsidiaries, operations and/or connections in China will have to see whether their onshore entities would be considered CIIOs, what type of data goes through their network, how such data and their network can be secured, and, if such data is important data, whether it can be transmitted outside China and whether it can pass the CAC-led security assessment. As financial services are designated as one of the crucial industries under the CSL and its implementation regulations, many players in this highly regulated industry have begun internal data mapping and other compliance analyses to assess the application of these requirements to them. In particular, whether they would need to formulate a data localisation plan for their China-generated data and implement compliance measures accordingly (Table 1).

Table 1: Examples of data requirements and compliance measures

Examples of data and cyber policies and documentation that companies adopt for China compliance
Data privacy policy
Internal management policy and operational protocol
Data classification policy
Data security management and access control policy
Cyber and data incident emergency plan
Data retention policy
Data processing register
Data subject request policy
Personal information protection impact assessment
Data export security assessment policy

Data Security Law

The DSL, which passed on 10th June, 2021 with effect from 1st September, 2021, governs data processing activities (ie the collection, storage, use, processing, transmission, provision and disclosure of data), security supervision and regulation of such activities within China.[23] It establishes a data classification and hierarchical data protection system, which consists of a data security risk assessment, monitoring and early warning mechanism as well as an incident response mechanism to prevent and mitigate any potential data security risk. It also sets out China's data security regulatory framework with a central leading national security authority at the top providing guidance and

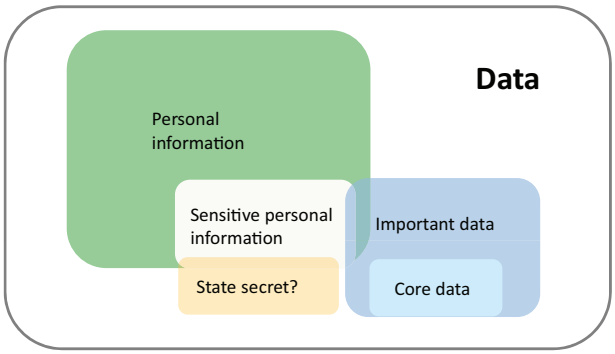


Figure 1 Types of data under the PRC laws

coordinating with local and other governmental departments on national data security strategy.

Data classification required

The data security mechanism consists, among other things, of the classification of data based on its importance in economic and social development as well as the extent of harm to national security, public interests or the lawful rights and interests of individuals and organisations, with 'core data' and 'important data' given prioritised protection.[24]

Figure 1 shows a high-level data classification chart based on various types of data discussed under the PRC laws.

On 14th September, 2022, China's chief technical standards committee released a draft national standard on requirements for classification and grading of network data.[25] Based on requirements under the draft national standards, Table 2 shows how the six impact objects and the three degrees of impact determine whether the data is 'general', 'important' or 'core'.

What is important data?

While a catalogue of important data will be formulated at the state level, each locality and governmental department will also come up with specific catalogues of important data for their respective region, department and relevant industries and sectors, and prioritise the data listed in the catalogues for protection.[26]

Guidelines and rules on what is considered important data are being issued or considered at the state level and even a few at the industry sector level. Companies are eagerly awaiting the publication of these catalogues to see how the DSL will affect their operations. And industry associations like ASIFMA and law firms such as Linklaters, representing global financial institutions, are trying to seek further clarifications or flexibilities from the relevant regulators so that these data-related laws and regulations can be applied in a practical way for different types of businesses.

What needs to be done with important data?

Handlers of important data have a slew of obligations under the DSL. They include: (a) conducting risk assessments regularly and submitting the risk assessment reports to competent authorities,[27] (b) enhancing risk monitoring and taking immediate remedies for any security bugs or vulnerabilities,[28] (c) responding quickly to any data breach and informing users and competent authorities in a timely manner,[29] (d) cooperating with legitimate requests for data retrieval by public security organs and national security

Table 2: Impact objects and their degrees of impact

	Degree of impact		
Impact object	*Particularly serious hazard*	*Serious hazard*	*General hazard*
National security	Core data	Core data	Important data
Economical operation	Core data	Important data	Important data
Social stability	Core data	Important data	General data
Public interest	Core data	Important data	General data
Organisational interests	General data	General data	General data
Personal interests	General data	General data	General data

organs,[30] and (e) designating a responsible person and an internal administrative unit responsible for data security to implement the data security protection obligations.[31]

The foregoing can be quite challenging and burdensome for most organisations, particularly global ones, in a market that has, until recently, not had a formal framework for data security and management.

What is core data?

The DSL also mentions 'core data', which refers to data in relation to national security, the lifeline of the national economy, important aspects of people's livelihood and major public interests.[32]

As with many Chinese laws, which are very high level with few details (which tend to be set out in subsequent implementing regulations), the DSL provides only that core data shall be administrated more stringently.[33] As a result, legal uncertainty remains for organisations in certain crucial industries or sectors where data of a sensitive nature is more likely to be processed and therefore any additional safeguards need to be understood by them to ensure effective implementation and compliance. These organisations will have to monitor closely for further clarification in this area.

What is required for cross-border transfer of data?

As under the CSL, the DSL requires that important data collected or generated by CIIOs be stored within the territory of China and, if necessary, to be transferred outside such territory and pass a security assessment by the State cyberspace authorities.[34] The DSL further provides that cross-border transfer of important data of non-CIIOs will be regulated by measures to be enacted by the State cyberspace authorities together with relevant departments of the State Council.[35] Those measures, known as the Measures on the Security Assessment for Cross-border Data Transfer (Security Assessment Measures)[36] were issued on 7th July, 2022 with effect from 1st September, 2022. As the Security Assessment Measures also cover cross-border transfers of personal information, they are discussed after the next section on the PIPL.

Sharing of data/information with foreign judicial or law enforcement agencies

Of particular interest to foreign companies is the requirement under the DSL that companies or individuals must *not* provide *any* data stored within the territory of China to overseas judicial or law enforcement bodies,

unless approved by the competent Chinese authorities.[37]

This, of course, gives rise to a conflict of law situation for foreign firms that may be required by their home jurisdiction to produce certain information from their China subsidiaries or other business presences but which they may not be able to do because of the approval requirement under the DSL and other Chinese laws and regulations. Indeed, in the absence of specific guidance on how to apply for an approval, which authority would be responsible for this approval, and how long the approval process may take, this provision of the DSL poses one of the key challenges for multinational businesses, particularly regulated ones such as those in the financial industry, that may be required to respond to requests for data from judicial or law enforcement bodies in their home jurisdiction.

Due to the vagueness of China's security laws and regulations, some businesses in China are declining to provide data to entities outside China, including their offshore parents or overseas shareholders, either because they want to err on the side of caution or because they want to avoid disclosure, particularly in sensitive situations where they know that it may be in response to regulatory investigations by authorities such as the US Securities and Exchange Commission or subpoenas from a US court, for example.[38]

Extraterritorial application of the DSL

Another point to note is the DSL provides that data handling activities conducted outside the territory of China that harm national security, public interests or legitimate rights and interests of citizens and organisations shall be held legally liable in accordance with the laws. While such an extraterritorial provision is not uncommon in other jurisdictions, such as under the EU's GDPR, it may be difficult to enforce in practice but nevertheless present a risk to foreign firms with a subsidiary or operations in China.

So far, there are no apparent instances of extraterritorial enforcement of the DSL, although the Chinese courts have sought to exert extraterritorial jurisdiction over at least one anti-monopoly dispute[39] this year based on the principle of extraterritorial application provided in the Anti-Monopoly Law.[40] There is an increasing trend of inclusion of extraterritorial provisions in China's new and amended laws and regulations, which is perhaps emblematic of the growing influence of China and its institutions in global business, with a resulting increase in compliance considerations for organisations dealing with China on a cross-border basis.

Personal Information Protection Law

Shortly after the issuance of the DSL, the PIPL was passed on 20th August, 2021, with effect from 1st November, 2021 to protect the rights and interests of individuals, promote the reasonable uses of personal information and regulate personal information processing activities, which includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, excluding anonymised information.[41]

Rights of individuals

Not unlike the personal data privacy laws in many jurisdictions, the PIPL establishes an individual's consent as the principal legal basis for handling personal information and an individual's rights to access, rectify, delete and/or transfer their personal information. As shown in Table 3, most of the PIPL's individual rights are GDPR-aligned. Nevertheless, unlike the GPDR, the PIPL does not specify conditions or exemptions

Table 3: A comparison of individual rights under PIPL and GDPR

Individual rights	*PIPL*	*GDPR*
Right to information	√	√
Right to access/obtain a copy	√	√
Right to correction/rectification	√	√
Right to erasure	√	√
Right to data portability	√	√
Right to object/restrict	√	√
Right related to automated decision making	√	√
Right to request explanation	√	×
Rights related to a deceased person	√	×
Right to lodge a complaint	√	√

that may apply to the exercise of individual rights and omits any procedure or specific timeline for responding to an individual's request with respect to their personal information. As a result, it remains to be clarified by the Chinese regulators as to how individual rights under the PIPL might be interpreted and enforced in practice.

Who are personal information processors?

Under the PIPL, personal information processors (PIPs) are entities and individuals processing or handling personal information autonomously.[42] They include foreign or offshore entities which process or handle personal information of individuals in China for the purpose of offering products or services to them or analysing and assessing their behaviours. But those who process or handle personal information for family or personal reasons are not subject to the PIPL.

What are the obligations of PIPs?

PIPs are required under the PIPL to abide by the principles of legality, fairness, good faith, minimum necessity (meaning that there should be specific and reasonable purposes for the processing of personal information), openness and transparency.[43]

PIPs, for example, must notify individuals prior to handling their personal information of (a) the name and contact details of the PIP, (b) the category or categories of personal information to be processed, (c) the purpose(s) of the processing, (d) the retention period (which should be the shortest period necessary) and (e) the ways for the individuals to exercise their data privacy rights.[44] In practice, PIPs tend to specify these required information through a privacy notice. International multinational businesses that have put in place GDPR-compliant or home jurisdiction-compliant privacy notices will need to seek local review of their privacy notices to identify what information must be supplemented to ensure compliance with the notice requirements under the PIPL.

PIPs may not process personal information without a lawful basis under the PIPL, which includes obtaining the individual's consent.[45] Where PIPs process personal information on the basis of the individual's consent, a higher consent standard, ie obtaining a 'separate consent', must be

obtained in certain circumstances, including for the export of personal information from China.[46] However, as the PIPL fails to specify what constitutes a 'separate consent', uncertainty remains as to how PIPs can satisfy this obligation in practice.

PIPs must also implement security measures to protect personal information from any unauthorised use or disclosure.[47] PIPs who process personal information of a certain amount have to appoint a personal information protection officer to be responsible for supervising the processing of such information and adopting protection measures[48] and, in some cases, even for establishing an independent body composed mainly of outside parties to supervise the protection of personal information. If the PIP is located outside China, it must appoint a representative in China (similar to the GDPR but the practical framework to comply with this requirement is yet to be implemented by the Chinese authorities) and conduct regular audits of the data handling.[49]

PIPs that process sensitive personal information, ie personal information that, once leaked or illegally used, may result in harm to the individual's dignity or personal or property security,[50] may not do so unless there are specific purposes and need, and strict protective measures have been adopted.

Cross-border transfers of personal information

A cross-border transfer of personal information includes not only the transfer or storage of China-generated personal information outside of China, but also the remote access to such information stored in China from an offshore jurisdiction.[51] Under the PIPL, PIPs who need to transfer personal information out of China generally have to provide prescribed information to, and obtain separate consent from, the individual and either (a) pass the security assessment by CAC, (b) execute a standard contract prescribed by CAC with the overseas recipient of such information, (c) obtain a personal information protection certification by specialised institutions recognised by the CAC, or (d) satisfy other conditions prescribed by laws.[52]

However, CIIOs and PIPs that process a large volume of personal information reaching the thresholds set out in the Security Assessment Measures must pass a security assessment by CAC.[53]

Security assessment

As mentioned in the previous section, the CAC Security Assessment Measures apply to (a) the transfer of important data, (b) personal information processed by CIIOs or by entities that hold over 1m individuals' personal information and (c) the transfer of more than 100,000 individuals' personal information or more than 10,000 individuals' sensitive personal information, accumulatively since 1st January, 2021.[54]

As a result, companies should establish a real-time monitoring mechanism to check the types and amount of personal information that they may or will export and to determine whether they need to apply for the data export security assessment. In practice, however, companies face difficulties with how to calculate the specific thresholds. For example, it remains to be clarified by the Chinese regulators as to whether all personal information disclosed in various data export applications made by one entity has to be aggregated, and whether the personal information of the same individual being transferred to two separate offshore recipients would be counted only once or be subject to double counting.

The security assessment process involves the submission to CAC of a self-assessment and a legally binding transfer agreement followed by a 45 working day review period, which may be extended for more complex cases that require supplementary materials.[55] It is important to note that the result of an assessment is valid only for two years[56]

so companies that want to transfer the same type of information cross-border will have to go through the security review process every two years.

CAC also released, on 31st August, 2022, its 'Application Guidelines on Data Export Security Assessment'[57] to guide in-scope organisations on how to complete their security assessments. However, given some apparent gaps in the guidance, uncertainty remains as to various practical aspects of the application process.

Sharing of information with foreign judicial or law enforcement agencies

As in the DSL, PIPs also must seek approval from the Chinese authorities if they have to provide any personal information they process that is stored in China to any overseas judicial or law enforcement authority. Like the challenges stated above, uncertainty remains for PIPs that receive a request for personal information from these overseas authorities.

DATA EXPORT CONSIDERATIONS AND WORKFLOW

For organisations that want or need to transfer onshore China data outside China, Figure 2 presents a chart of the high-level considerations and workflow based on the aforementioned laws and regulations that may be helpful.

IMPLICATIONS FOR FOREIGN COMPANIES WITH CONNECTIONS TO CHINA

Foreign companies with operations or subsidiaries in China or dealings with entities or individuals in China should determine how the aforementioned data-related laws and regulations affect them as cross-border data flows and sharing of information can be expected in today's global business environment.

Different types of data/information and what can be shared/transferred abroad?

For example, if a foreign company has a majority or wholly-owned subsidiary in China, it would want to have access to its subsidiary's (i) corporate information (eg board resolutions and meeting minutes, management reports, corporate policies and procedures) for governance purposes, (ii) financial and accounting information for financial oversight as well as consolidation purposes, (iii) employee information for resource allocation, internal controls and oversight purposes and (iv) vendor and service provider information for risk management, internal controls and potential cost savings purposes.

If the foreign company is a listed or regulated company, it would probably need even more information to meet its own regulatory compliance and disclosure obligations and to demonstrate that it is able to exercise proper oversight over its China subsidiary. Such information may include (a) client or customer information of the subsidiary for risk management, know your client, anti-money laundering (AML)/counter terrorist financing (CFT) and sanctions screening purposes, (b) broker and securities transaction information for counterparty risk management, best execution monitoring as well as internal controls and compliance purposes and (c) listed companies' shareholding information for concentration risk monitoring and disclosure of interest reporting purposes.

If the foreign company is a global asset management company, it would want to have access to its China subsidiary's research and analyses of the Chinese economy, market, industries and specific companies in order to benefit from the local knowledge and expertise of its analysts in China, align its onshore and offshore strategies and ensure consistency of the group's investment approach towards China.

However, even without research being deemed as important data, the CSRC's

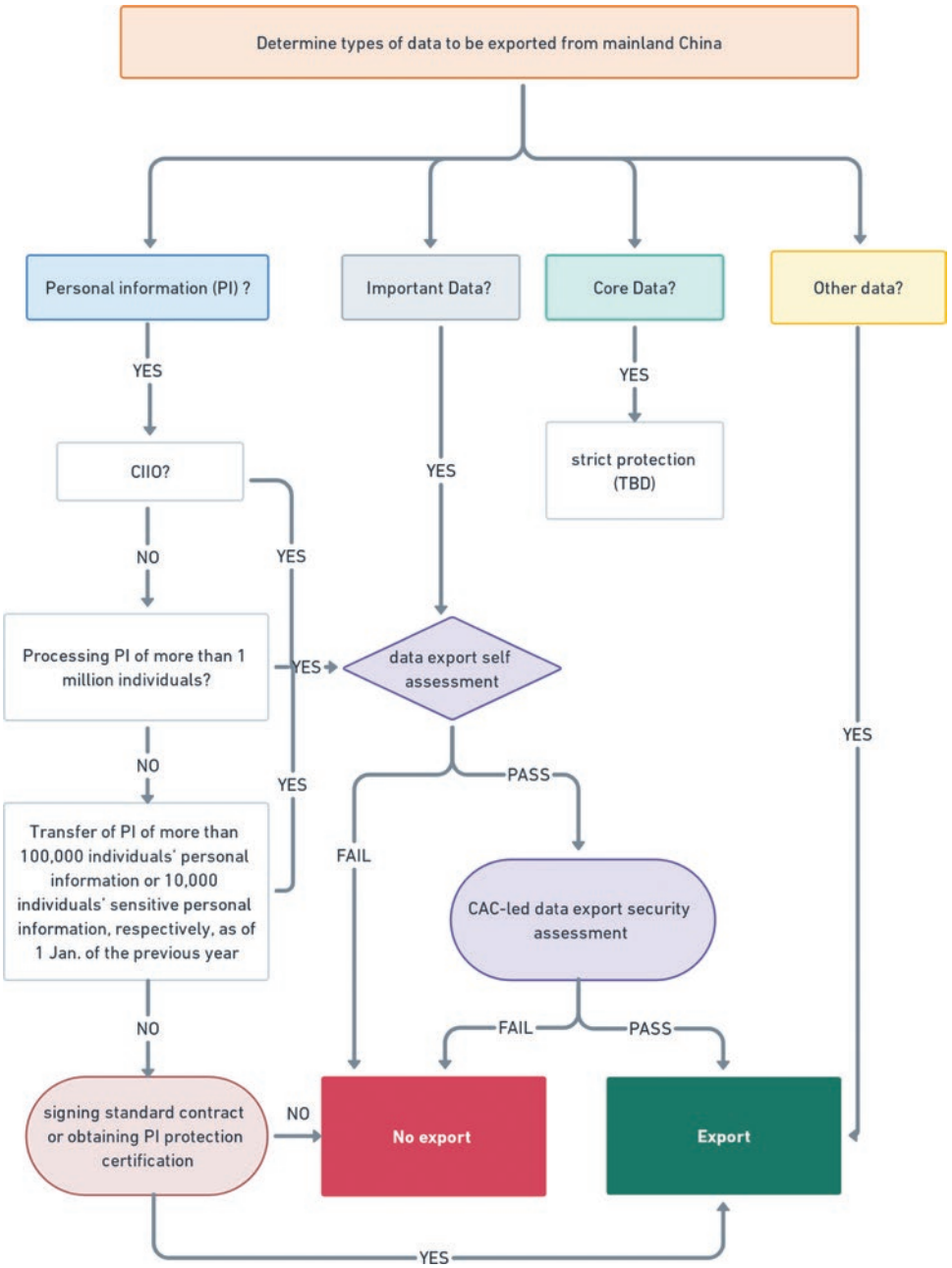


Figure 2 Data export mechanisms flowchart

'Measures for the Supervision and Administration of Publicly-Offered Securities Investment Fund Managers'[58] require that public fund management companies segregate 'key information' between its business and clients from that of its shareholders and such a requirement has been the basis for the refusal by many China fund management companies to share their research and other information with their overseas parent.

Somewhat counter-intuitively, if the same research analysts work at a registered private

fund manager or an unlicensed China consultancy entity conducting financial markets research in China (often for an overseas parent or affiliate), the research can be exported to the overseas parent or affiliate with considerably less or no restriction. It would be helpful for the regulations on the cross-border sharing of research in the financial sector to be aligned.

In addition, the 'Guidelines for the Governance of Securities Investment Fund Management Companies'[59] issued by the CSRC on 15th June, 2006 specifically state that the shareholder of a fund management company shall not, directly or indirectly, request the company to provide non-public information or materials on fund investment and research.[60]

These data sharing restrictions greatly diminish the value of foreign-owned public fund management companies in China as the China staff of these companies will not be able to benefit from the knowledge, experience and expertise of the group acquired in other markets while the group also will not be able to leverage the knowledge, experience, and expertise of its China entity. They also reduce the value that foreign-owned public fund management companies can bring to Chinese investors by offering them exposure to global perspectives, investment strategies and best practices.

What should foreign companies and their China affiliates do to ensure compliance with data sharing rules?

Before transferring data generated or stored in China to a third jurisdiction, foreign companies with China operations, subsidiaries, affiliates or other China connections may want to, together with their China affiliates:

(a) conduct a data mapping exercise to understand their key data flows, including, for example, to review the type of data they need from China (in particular, whether personal information is involved), the purposes and means of transfer, the nature of the offshore data recipients and the location where data is stored and is to be stored;
(b) determine whether that data falls within the scope of regulated data, in particular, important data, core data, or data subject to industrial export restrictions (such as in the finance industry);
(c) determine whether the China entity is a CIIO or a PIP that reaches the personal information thresholds set out in the Securities Assessment Measures;
(d) if the answer to (b) or (c) is yes, be prepared to apply for a security assessment and/or seek prior government approval, including conducting a data export self-assessment in accordance with the Securities Assessment Measures and taking remediation actions to address issues identified that could affect data export security, and entering into binding legal documentation such as a data transfer agreement with offshore data recipients; and
(e) if the answer to (b) or (c) is no, follow one of the other two available transfer mechanisms, ie either enter into a standard contract (the final draft of which remain to be published by the CAC) for cross-border transfers of personal information or obtain a personal information protection certification by specialised institutions recognised by the CAC, and fulfil other requirements under the PIPL (such as providing necessary notices and obtaining separate consents when relying on consent for the exports of personal information).

What to do in a conflict of law situation?

The inability to access or obtain certain information from its China subsidiaries or other business presences due to Chinese laws and regulations may put a foreign parent or shareholder in a difficult position, as it may result in the latter being in breach

of its home jurisdiction regulations and legal obligations.

For example, to prevent money laundering and terrorist financing globally, the Financial Action Task Force (FATF) developed the FATF Recommendations or Standards[61] that over 200 countries (including China) and jurisdictions have committed to implement. Among them is Recommendation 18, which provides that financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing within the group for AML/CFT purposes. It provides further that financial institutions should be required to ensure that their foreign branches and subsidiaries apply the AML/CFT measures consistent with the home country requirements of the parent or group implementing the FATF Recommendations.

If a foreign financial institution is unable to monitor the AML/CFT policies and practices of its China subsidiary, this would be a serious issue for them, as most financial institutions, such as banks, are subject to strict requirements in this area.

Other countries and jurisdictions have similar requirements that expect overseas branches and subsidiaries of their banks and financial institutions to apply AML/CFT measures consistent with their parent's requirements or programme against money laundering and terrorist financing. To effectively assess and monitor their overseas branches' and subsidiaries' compliance with such requirements or programmes, banks and other financial institutions must have access to certain information, such as client due diligence information, compliance reports or reports of breaches to onshore regulators as well as the opportunity to inspect those subsidiaries.

Another conflict of law example involves the disclosure and reporting of shareholdings in listed companies. Many jurisdictions, including China, require the aggregation and disclosure of shareholdings of the group in a listed company. If the China subsidiary is not allowed to share its shareholding in a listed company that is listed in more than one jurisdiction (such as Hong Kong or the US) with its offshore parent, the offshore parent may be in breach of its own disclosure of interest obligations in those other jurisdictions.

ASIFMA has been highlighting to Chinese regulators the reasons why some onshore China data is needed by global financial institutions for risk management, internal controls and compliance purposes, as well as the conflict of law situation created when such data is not allowed to be shared outside China. It is hoped that the catalogues of important data and guidelines being drafted by Chinese regulators will consider the legitimate needs for such data and strike a balance between such needs and the protection of relevant data.

Law firms such as Linklaters have been assisting international companies in assessing whether the China authorities' approval must be obtained and, if so, how to obtain such approval, before their Chinese subsidiaries can provide certain data to their overseas parent, especially in response to regulatory or investigatory queries from foreign governmental authorities. Although there is no one-size-fits-all solution to dealing with information requests, in practice it would be helpful to assess the location of where the requested data is stored, the categories, nature and volume of data requested, and the nature of the query received from the foreign regulator etc. Case-by-case analysis is recommended in most instances.

CONCLUSION

The need for jurisdictions to develop regulatory frameworks is understood, in order to protect personal information and certain types of data, and to promote the safe and free movement of personal and non-personal

data across borders. Financial data, including personal and non-personal data, is pivotal to financial institutions, particularly global ones, and, thus, the protection of the processing of such data and the safe and free movement of such data across borders are essential to maintaining the integrity of financial markets and confidence of market participants, including investors and customers.

Cross-border data transfer requirements under China's three-pillar data laws — the CSL, DSL and PIPL — are an important component of the regulatory regime of personal information protection and non-personal data regulation. However, cross-border sharing of information located in China is, and will remain, the biggest challenge for foreign institutions with subsidiaries and/or operations in China until there is more clarity on a number of outstanding questions. For example, what kinds of data are considered important data by the Chinese authorities, under what circumstances may such data be shared and how China's concerns over national security, data protection and data security can be addressed without impeding legitimate business needs, particularly for the financial industry, which often involves a lot of cross-border transactions and activities.

Businesses undertaking cross-border business with China should — if they have not done so already — assess their data flow arrangements as soon as possible and the impact of regulatory developments in China on their business operations. They are likely to have to upgrade their compliance programmes to comply with these data regulations and pay close attention to the applicable industry-level regulations, rules and guidelines released by their respective supervisory authorities (such as, in the case of financial institutions, the People's Bank of China, China Banking and Insurance Regulatory Commission and the CSRC), given the potential overlapping areas of regulation.

It may be useful for foreign institutions with long-term interests in continuing to operate, or invest in, or have dealings with the Chinese market to work through their own government and/or home regulator, chambers of commerce and industry associations to convey their challenges so that the right balance between protecting national and public interests and facilitating cross-border investments and business exchanges can be achieved.

Finally, there is a question as to whether it is the regulatory authorities in the various jurisdictions, which often have memorandum of understanding or cooperation agreements signed with each other, that should try to come to an agreement on more effective channels for legitimate information exchange that minimise uncertainty and delay rather than leave companies in a conflict situation.

AUTHORS' NOTE

The authors would like to thank Tiantian Ke, Associate, Linklaters Zhao Sheng and Luming Liang, Senior Associate, ASIFMA Asset Management Group for their support in preparation of this paper.

References

(1) 'Data Security Law of the People's Republic of China' (DSL), passed on 10th June, 2021, with effect from 1st September, 2021, available at: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed 20th September, 2022).

(2) 'Personal Information Protection Law of the People's Republic of China' (PIPL), passed on 20th August, 2021, with effect from 1st November, 2021, available at: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed 20th September, 2022).

(3) 'Cybersecurity Law of the People's Republic of China' (CSL), passed on 7th November, 2017, with effect from 1st June, 2017, available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (in Chinese). An unofficial translation is available at: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (accessed 20th September, 2022).

(4) Article 1 of the CSL.
(5) Article 2 of the CSL.
(6) Article 76 (1) of the CSL.
(7) Article 76 (3) of the CSL.
(8) Article 12 of the CSL.
(9) Article 21 of the CSL.
(10) Article 40 of the CSL.
(11) Article 28 of the CSL.
(12) Article 23 of the CSL.
(13) Article 34 of the CSL.
(14) Article 37 of the CSL.
(15) *Ibid*.
(16) Article 35 of the CSL.
(17) Article 36 of the CSL.
(18) 'Regulations on Critical Information Infrastructure Security Protection', issued by the State Council on 30th July, 2021, with effect from 1st September, 2021, available at: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (in Chinese). An unofficial translation is available at: https://www.chinalawtranslate.com/en/Regulations-on-Critical-Information-Infrastructure-Security-Protections/?tpedit=1 (accessed 20th September, 2022).
(19) Article 2 of the Regulations on Critical Information Infrastructure Security Protection.
(20) *Ibid*.
(21) Articles 9 and 10 of the Regulations on Critical Information Infrastructure Security Protection.
(22) Article 10 of the Regulations on Critical Information Infrastructure Security Protection.
(23) Articles 2 and 3 of the DSL.
(24) Article 21 of the DSL.
(25) 'Information Security Technology – Requirements for Classification and Grading of Network Data' (Draft for Public Consultation), available at https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220914180530&norm_id=20211108000024&recode_id=48416 (in Chinese only) (accessed 4th November, 2022).
(26) Article 21 of the DSL, ref 24 above.
(27) Article 30 of the DSL.
(28) Article 29 of the DSL.
(29) Article 23 of the DSL.
(30) Article 35 of the DSL.
(31) Article 27 of the DSL.
(32) Article 21 of the DSL, ref 24 above.
(33) *Ibid*.
(34) Article 36 of the DSL.
(35) Article 31 of the DSL.
(36) 'CAC's Measures on the Security Assessment for Cross-border Data Transfer (Security Assessment Measures) issued on 7th July, 2022, with effect from 1st September, 2022, available at: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (in Chinese only) (accessed 20th September, 2022)
(37) Article 36 of the DSL, ref 34 above.
(38) See re Valsartan, Losartan and Irbesartan Prod. Liab. Litig., No. MDL 2875 (RBK), 2021 WL 6010575, at *10 (D.N.J. Dec. 20, 2021); Philips Med. Sys. (Cleveland) *v*. Buan, 19 CV 2648 (N.D. Ill. Mar. 1, 2022).
(39) Case No. 392 [2020], Zhi Min Jurisdiction Final, the Supreme People's Court.
(40) 'Anti-Monopoly Law of the People's Republic of China' issued 30th August, 2007 and amended on 24th June, 2022, available at: http://www.gd.gov.cn/zwgk/wjk/zcfgk/content/post_2521388.html (in Chinese only) (accessed 4th September, 2022).
(41) Article 4 of the PIPL.
(42) Article 73 of the PIPL.
(43) Articles 5 and 7 of the PIPL.
(44) Article 17 of the PIPL.
(45) Article 13 of the PIPL.
(46) Article 39 of the PIPL.
(47) Article 51 of the PIPL.
(48) Article 52 of the PIPL.
(49) Article 53 of the PIPL.
(50) Article 28 of the PIPL.
(51) Article 1 of the 'Application Guidelines on the Data Export Security Assessment', issued by the CAC on 31st August, 2022, available at: http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm (in Chinese only) (accessed 20th September, 2022).
(52) Article 38 of the PIPL.
(53) Article 40 of the PIPL.
(54) Article 4 of the Security Assessment Measures.
(55) Articles 5 and 12 of the Security Assessment Measures.
(56) Article 14 of the Security Assessment Measures.
(57) CAC's 'Application Guidelines on the Data Export Security Assessment', issued on 31st August, 2022, available at http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm (in Chinese only) (accessed 20th September, 2022).
(58) Article 33 of CSRC's 'Measures for the Supervision and Administration of Publicly-offered Securities Investment Fund Managers', issued on 20th May, 2022, with effect from 20th June, 2022, available at: http://www.csrc.gov.cn/csrc/c101953/c2804634/content.shtml (in Chinese only) (accessed 20th September, 2022).
(59) CSRC's 'Guidelines for the Governance of Securities Investment Fund Management Companies', issued on 15th June, 2006, available at: http://www.gov.cn/zwgk/2006-06/23/content_317785.htm (in Chinese only) (accessed 20th September, 2022).
(60) Article 19 of the 'Guidelines for the Governance of Securities Investment Fund Management Companies'.
(61) 'FATF Recommendation International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation', issued in February 2012 and last updated in March 2022, available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed 20th September, 2022).