15 October 2023

To: Cyberspace Administration of China ("**CAC**")

CC:
National Administration of Financial Regulation, No.15 Financial Street, Xicheng District, Beijing, 100033
People's Bank of China, 32 Cheng Fang Street, Xi Cheng District, Beijing, 100800
China Securities Regulatory Commission, 19 Jin Rong Street, Xi Cheng District, Beijing 100033

Re: ASIFMA's Response to the Consultation Draft of the Provisions on Regulating and Promoting Cross-Border Data Flows

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**") [1]("we", "our" or "us") are pleased to submit to CAC our comments and suggestions on the Provisions on Regulating and Promoting Cross-Border Data Flows ("**Draft Provisions**") released on September 28.

This letter sets out the views of ASIFMA's members on the Draft Provisions and suggestions for further clarification on and adjustment of the current clauses of the Draft Provisions.

We understand the need for jurisdictions to develop regulatory framework protecting data security and personal information and promoting safe and free cross-border data flow, which is pivotal to the business of our members, and more broadly, essential to the integrity of international financial markets and customer and business confidence. As such, we welcome the recent release of the Draft Provisions and fully support the finalization and issuance of the rules embodied therein. By providing our comments and suggestions for the Draft Provisions, we hope to drive consensus, advocate solutions for issues discussed under the Draft Provisions through our collective strength and clarity of one industry voice, and hope that our suggestions may contribute to the further development of the regulatory mechanism for outbound data transfer activities of the PRC. ASIFMA and its members remain committed to engage

[1] ASIFMA is an independent, regional trade association with over 170 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive, and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the Global Financial Markets Association ("GFMA") alliance with the Securities Industry and Financial Markets Association ("SIFMA") in the United States and the Association for Financial Markets in Europe ("AFME"), ASIFMA also provides insights on global best practices and standards to benefit the region.

further and to share our collective knowledge and observations.

Our detailed considerations and suggestions in relation to the Draft Provisions are highlighted in the schedule to this letter. We very much appreciate the opportunity to respond to the Draft Provisions and look forward to engaging in further communication with CAC and any other relevant bodies as may be helpful.

Should you have any questions in relation to this letter or would like to obtain further industry input, please contact Diana Parusheva, Executive Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

We will also share a copy of our submission with the PBOC, NAFR and CSRC, given the potential overlapping areas of regulation.

Sincerely,

Diana Parusheva-Lowery
Executive Director – Head of Public Policy and Sustainable Finance
Asia Securities Industry & Financial Markets Association (ASIFMA)
www.asifma.org

Schedule

Part A General Comments and Suggestions

1. Scope of "Important data"

Whilst the Draft Provisions have provided specific exemptions for outbound PI transfer, no special exemption has been provided for the outbound transfer of important data. It is therefore important to give special consideration on outbound data transfer commonly involved in or necessary for the operation of development of cross-border business (as the ones we discussed under below Sections 3.2-3.8), when determining the scope of the important data.

ASIFMA suggestion: CAC to consider, via coordination with and suggestion to the competent industrial regulators (for the financial industry, mainly the NAFR, CSRC and POBC), providing sufficient room for outbound data transfer under scenarios set out in below Sections 3.2- 2.8, by defining a well-tailored and narrow scope of "important data". It is also recommended that CAC simplify transfer of data frequently involved in the cross-border financial business scenarios such as AML/KYC related data, when formulating the important data catalogue for the financial industry.

2. Application thresholds

The Draft Provisions have, via Clause 5 and 6, set forth new application thresholds for outbound personal information ("**PI**") transfer activities related regulatory requirements, i.e., outbound PI transfer will be subject to:

- security assessment requirement, if PI to be transferred offshore within 1 year is expected to be of no less than 1 million individuals; or
- standard contract ("**SCC**") filing or PI protection certification requirement, if PI to be transferred offshore within 1 year is expected to be of more than (inclusive) 10,000 individuals, but less than 1 million individuals.

(security assessment, China SCC filing and PI protection certification are hereinafter collectively referred to as the "**Export Mechanism**")

However, the Draft Provisions provide no further guidance on (i) the timing for making of the estimate, (ii) the calculation method of the "1 year" period (i.e., what is the starting point for calculating "within one year); and (iii) whether data exempted from the Export Mechanism under the Draft Provisions shall still be counted when calculating the 10,000 & 1 million thresholds.

ASIFMA suggestion: CAC to consider adding specific guidance in the Draft Provisions on the calculation method of the "1 year" period and the quantity thresholds, by (i) setting forth a clear cut-off date for the estimation of data quantity; (ii) adopt a calendar year based calculation approach so that it is feasible to operationalize, and (iii) specifically excluding exempted PI transfer from the calculation.

Clarification is also required as to whether the exempted PI transfer shall still be disclosed in the application documents for the Export Mechanism, e.g. PIPIA report.

3. Regulatory measures for outbound data transfer under special scenarios

Whilst the Draft Provisions have substantially lifted regulatory barriers for outbound data transfer, we note there are certain scenarios of particular concerns in international institutions' data compliance management, that have been not specifically addressed under the Draft Provisions. These scenarios include:

3.1 Outbound data transfer by onshore representative offices and branches of foreign entities

As a matter of practice, application for SCC filing by onshore representative offices or branches are generally rejected at provincial level on the ground that these presences are not considered "independent entities" under PRC law. This has led to the question as to how shall such entities ensure regulatory compliance when data to be transferred offshore by them meets the application threshold for SCC filing.

ASIFMA suggestion: CAC to consider providing clarification for the applicable regulatory mechanism for outbound data transfer by onshore representative offices, branches or other types of entities that do not have an "independent" legal status.

3.2 Outbound transfer of personal information of legal/authorized representative, senior management, individual shareholders, ultimate beneficiary owner, designated contact persons and individual signatory, as well as business contact information

Name, title, phone number, email address as well as other basic information of legal/authorized representative, senior management, individual shareholders, ultimate beneficiary owner, designated contact persons and individual signatory, (as well as other business contact information) of onshore and offshore entities, constitute a major part of data involved in cross-border data flow in the normal operation of international/cross-border business, and are normally viewed as part of the basic information of the related entities and thus encouraged or required to be disclosed to the public to ensure business transparency and integrity; and given the role of the relevant data subjects, the disclosure and further handling of such information in cross-border business context are likely to fall within the reasonable expectation of the data subjects.

ASIFMA suggestion: CAC to consider setting forth special exemption clause for outbound transfer of PI of legal/authorized representative, senior management, individual shareholders, ultimate beneficiary owner, designated contact persons, individual signatory, and other individuals with similar title/position, as well as other business contact information.

3.3 Outbound data transfer for risk management and compliance monitoring purpose

For international group companies, in order to implement risk management and compliance check, offshore headquarters or parent companies would need to obtain operational & compliance data (including, in particular, employee data and business data) of their onshore affiliates for internal

assessing and filing purpose. These data may involve PI of onshore prospects, clients, employees and/or third party contractors, and subject to the onshore operation scale, may exceed the 10,000 individual threshold. Outbound PI transfer under such scenarios are normally viewed as of substantial necessity in cross-border business operation for global firms.

ASIFMA suggestion: CAC to consider setting forth exemption clause for inner group outbound transfer of personal information necessary for risk management and compliance monitoring purposes.

3.4 Outbound data transfer for operational, transactional and management purposes

International group companies normally face the need to access and review the data of their overseas affiliates, clients and counterparties (including those located in China) during their business operation and transactional activities, especially where centralized resources are used for operational and management purposes (such as corporate governance, business evaluation and service provisions) or where a cross-border transaction is pursued. Outbound PI transfer under such scenarios are inevitable in the context of international business operation and development.

ASIFMA suggestion: CAC to consider setting forth exemption clause for outbound PI transfer necessary for global operational, transactional and management purposes, such as corporate governance, business evaluation, service provision and cross-border transactions.

3.5 Outbound data transfer for offshore litigation, arbitration or other legal proceeding purposes.

The Draft Provisions are silent on the application of Export Mechanism under offshore litigation or arbitration related outbound data transfer scenarios, where an onshore data handler is required to provide information in an offshore tribunal as a plaintiff, defendant, third party, witness and etc.

ASIFMA suggestion: CAC to consider providing clarification on the applicable rules and regulatory mechanism for outbound data transfer under offshore litigation, arbitration or other similar legal proceedings, either in the Draft Provisions or the legislative notes to be issued jointly with the finalized Draft Provisions (if any).

3.6 Outbound data transfer for offshore regulatory compliance purposes.

International companies/groups having local presence or business in China often face need for cross-border data transfer, due to regulatory compliance requirements (for example, the KYC/AML) in other jurisdictions. Whilst we fully understand the sensitivity of outbound data transfer under this scenario, given that under certain circumstances, outbound data transfer for regulatory compliance purpose is substantial important and necessary for the normal operation of an international company/group, a clear guidance on the compliance parameters would be highly appreciated by the market.

ASIFMA suggestion: CAC to consider adding separate clause(s) or special legislative notes for outbound data transfer required for offshore regulatory compliance such as KYC/AML, (i) specifying that the application thresholds set forth under the Draft Provisions apply to this scenario; and (ii) where

feasible, providing further details on the applicable regulatory mechanism and compliance parameters for relevant outbound data transfer activities.

3.7 Outbound transfer of publicly disclosed data

Publicly disclosed data (including personal information legally disclosed to the public, especially those published on the official government website) are less sensitive and therefore qualified for more flexible regulation.

ASIFMA suggestion: CAC to consider setting forth special exemption clause for the outbound transfer of publicly disclosed data.

3.8 Outbound transfer of pre-investment due diligence, investment research, portfolio data and other information collected in relation to stewardship activities that (after being transferred offshore) will only be shared within the group or disclosed to the relevant investors.

The operation and development of cross-border assets management and equity investment business, as well as cross-border strategic investment and M&A deals, normally involves cross-border transfer of pre-investment due diligent data, investment research, portfolio data and other stewardship activities-related data, which, after being transferred offshore, will only be handled for limited business purposes and provided to a limited group of parties.

ASIFMA suggestion: CAC to consider providing further flexibility or exemption for outbound data transfer under such scenario.

4. Post-transfer regulation and non-retroactive application

It's unclear under the Draft Provisions as to whether and what types of regulatory actions will be triggered if after the data is transferred, (i) the actual exported PI appears to exceed the estimated amount and thus meets the application threshold(s) of the Export Mechanism; or (ii) any of the exported data is later identified as important data in any post-transfer regulatory announcement or catalogue.

ASIFMA suggestion: CAC to consider, in addition to current Clause 9 and Clause 10, inserting specific clause or providing clarification on post-transfer regulation to avoid legislation uncertainties that may arise from future regulatory development. In particular, to protect and ensure regulatory consistency, stability and predictability, it is recommended to (i) allow certain flexibility where actual exported PI exceeds but not substantially differs from the estimated amount. e.g., specify that post-transfer regulatory measures will only be triggered whether the actual exported PI exceeds 125% of the estimated amount; (ii) make it clear that no retrospective administrative measures or penalties will be imposed on pervious data transfer activities.

5. Regulatory implementation before the formal issuance of the Draft Provisions

Given the Draft Provisions have substantially amended the application rules of Export Mechanism, for

onshore data handlers that are in the process of applying for the security assessment or SCC filing, onshore data handlers need to re-assess export mechanisms applicable to them after the formal issuance of the Draft Provision. Given the impact analysis and application related works (such as document preparation and communications) could be time-consuming, it could be reasonable and practical to provide a grace period for onshore data handlers to implement applicable Export Mechanisms for cross-border data transfers.

ASIFMA suggestion: CAC to consider (i) pausing the implementation of the Export Mechanism until the Draft Provisions takes effect; (ii) (after the issuance of the Draft Provisions) providing a grace period of at least 6 months for onshore data handlers to operationalize the new regime, and (iii) accelerating the issuance of the Draft Provisions, to avoid regulatory uncertainty.

Part B Comments on Specific Clause

In addition to the comments raised in Part A, we set forth in the table below our comments and suggestions with respect to specific clauses of the Draft Provisions.

Cl No.	Content	Comments	Suggestions
1	Where data is exported as a part of activities relating to international trade, academic cooperation, cross-border manufacturing and production, marketing activities and etc., does not contain personal information or important data, it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification.	➢ Based on the current clauses of the Draft Provisions, it appears that outbound data transfer will only be subject to the Export Mechanism if the transfer involves important data or PI, regardless of the scenarios involved. If this is the regulatory intention, it may be better to make it clear in this Clause 1, as current wordings of this clause seems to indicate otherwise.	• CAC to consider revising the current wordings as below: "*Where data to be exported ~~is exported as a part of activities relating to international trade, academic cooperation, cross-border manufacturing and production, marketing activities and etc.,~~ does not contain personal information or important data, it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification, unless otherwise provided under these provisions, laws and administrative regulations*"
2	Data handlers are not required to apply for export security assessment for important data export if data to be exported have not been notified or publicly declared as important data by the relevant authorities or regions.	➢ Please to refer to our comments in "Part A-Post-transfer regulation". ➢ It may be better to make it clear in this clause that important data will only be determined via catalogue or announcement officially and formally made, excluding those in consultation draft status .	• Please to refer to our suggestion in "Part A-Post-transfer regulation". In particular, CAC to consider providing clarification on applicable post-transfer regulatory measures for outbound data transfer where any of the exported data is later identified as important data.

Cl No.	Content	Comments	Suggestions
			• CAC to consider revising the current wordings as below: "*Data handlers are not required to apply for export security assessment for important data export if data to be exported have not been formally notified or ~~publicly~~ declared as important data by the relevant authorities or regions*".
3	If the personal information provided overseas was not collected or generated within the territory, it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification.	➢ We note Article 2 of the Measures for the Security Assessment of Outbound Data Transfer has provided certain clarification as to the scope of "onshore data", and would recommend CAC to adopt a consistent and balanced approach in relation of the application of this clause, and not to over-regulate data involved in offshore and cross-border operation and commercial activities.	• CAC to consider adopting a balanced approach for the implementation of this clause, so as to provide sufficient room and flexibility for data flow in globalized business operation and commercial cooperation. • CAC to consider revising the clause as below: *"If the personal information provided overseas was not collected or generated within the territory of PRC, it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification. "*
4	If one of the following circumstances is met, there is no need to declare a data export security assessment, enter into a personal information	➢ It is recommended to, when identifying scenarios that may fall within the exemption scope under this clause (such as those	• CAC to consider: - adopting a balanced approach for the application of exemptions provided in

Cl No.	Content	Comments	Suggestions
	export standard contract, or obtain a personal information protection certification: (1) Where it is necessary to provide personal information overseas to conclude or perform a contract to which the individual is a party, such as cross-border shopping, cross-border remittance, air ticket or hotel bookings, and visa applications, etc. (2) Where it is necessary to provide overseas the personal information of an internal employee for human resources management purposes in accordance with labour regulations established by law and collective contracts signed in accordance with law. (3) Where it is necessary to provide personal information overseas in order to protect the life, health and property of a natural person, etc., in an emergency situation.	"necessary" for the listed purposes or "in an emergency situation"), give consideration to outbound data transfer commonly involved or generally required in the operation of international companies and cross-border transactions (such as scenarios set out in above Part A-3), and providing sufficient room for normal business operation and development in the context of globalization and openness. ➢ In terms of sub-clause (1), - further clarification is required on: ▪ whether the exemption applies outbound PI transfer (i) under cross-border client referral arrangement; or (ii) due to cross-border outsourcing (where service is provided by the onshore outsourcer to the individual). ▪ whether the contracting individual needs to be the PI subject (e.g., information of family members of the contracting individual may be required under cross-border service scenarios) - where the contractual party is an entity (e.g., an onshore institutional client), for contractual performance purpose, personal information of the affiliated	this clause; - revising sub-clause (1) as below: *"Where it is necessary to provide personal information overseas to conclude or perform a contract to which the individual is a party, or to which the entity for which the individual serves in a leadership, management, membership, employment or ownership capacity, such as cross-border shopping, cross-border remittance, air ticket or hotel bookings, and visa applications, etc."* - revising sub-clause (2) as below: *"Where it is necessary to provide overseas the personal information of following individuals for human resources management purposes, including:* *(i)* employees *(ii)* interns; *(iii)* assignees/personnel from other entities within the group, or personnel dispatched by a third party; *(iv)* job applicants; *(v)* above individuals whose contract

Cl No.	Content	Comments	Suggestions
		individuals (such as the legal representative, senior management and other employees) of the entity may need to be provided offshore. However, the type of outbound data transfer, whilst with similar contractual necessity, is not exempted in this clause. ➢ In terms of sub-clause (2), - further clarification is required on whether the exemption applies to outbound transfer of (i) information of family members of the employees due to HR management purpose; (ii) candidate and third-party dispatch personnel data for global HR assessment purpose; and (iii) employee data due to offshore hosting and use of centralized HR resources, or for inner-group management purpose. - the qualifier "by law and collective contracts" is too narrow for required outbound data transfer under normal HR management.	*has expired or been terminated; and* *(vi) family members of the above individuals.* - Adding further exemption for outbound transfer of ▪ personal information of legal/authorized representative, senior management, individual shareholders, ultimate beneficiary owner, designated contact persons or individual signatory, as well as other business contact information; ▪ personal information for risk management and compliance monitoring purpose; ▪ personal information for global corporate governance, business evaluation, service provision, cross-border transactions and other global operational, transactional and management purposes; ▪ pre-investment due diligence, investment research, portfolio data and other information collected in relation to stewardship activities;

Cl No.	Content	Comments	Suggestions
			▪ publicly disclosed data; ▪ the individual loan identification number included in the packaged assets involved in the asset securitization business of the financial institutions; ▪ personal information incidentally transferred in the provision of technical support to local systems by the headquarters of a multinational company during an emergency (such as breaking glass access to restore a system); ▪ personal information transfers that have been approved in accordance with Article 41 of the PIPL; and ▪ PI transfer that is necessary for regulatory compliance or performing duty specified under applicable laws, regulations or other regulatory rules or requirements; or otherwise approved or confirmed by competent industrial regulators (such as the CSRC, NAFR and PBOC).
5	If it is estimated that personal information of less than 10,000 individuals would be provided overseas within one year, it is not necessary to	We recommend clarifying the following:	• CAC to consider revising this clause as follows: *If it is estimated that personal information*

Cl No.	Content	Comments	Suggestions
	declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification. However, where the personal information is exported overseas based on an individual's consent, consent must still be obtained from the personal information subject.	- the volume determination excludes the scenarios in Articles 3 and 4; - "one year" refers to the next calendar year; and - in the scenarios where personal information is indirectly collected (e.g., Business-to-Business scenarios), consent should be collected and provided by the entity that provides the personal information to the Data Processor.	*of less than 10,000 individuals would be provided overseas within ~~one year,~~ the next calendar year (excluding the scenarios in Articles 3 and 4), it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification. However, where the personal information is exported overseas based on an individual's consent, consent must still be obtained from the personal information subject; provided that if the data is collected by the Data Processor indirectly from individuals or organizations, the data provider shall be required to obtain the consent of the individuals or organizations in accordance with laws and administrative regulations.*
6	If it is estimated that personal information of more than 10,000 but less than 1 million individuals would be provided overseas within one year, and where (i) a personal information export standard contract has been concluded with the offshore recipient and filed with the local provincial cyberspace department, or (ii) the personal information protection certification has been	We recommend clarifying the following: - the volume determination excludes the scenarios in Articles 3 and 4; - "one year" refers to the next calendar year; and - in the scenarios where personal information is indirectly collected (e.g., Business-to-	• CAC to consider revising this clause as follows: *If it is estimated that personal information of more than 10,000 but less than 1 million individuals would be provided overseas within ~~one year,~~ the next calendar year (excluding the scenarios in Articles 3 and 4), and where (i) a personal*

Cl No.	Content	Comments	Suggestions
	obtained, it is not required to declare a data export security assessment. If personal information of more than 1 million individuals will be provided overseas within one year, a data export security assessment shall be declared. However, where the personal information is exported overseas based on an individual's consent, consent must still be obtained from the personal information subject.	Business scenarios), consent should be collected and provided by the entity that provides the personal information to the Data Processor.	*information export standard contract has been concluded with the offshore recipient and filed with the local provincial cyberspace department, or (ii) the personal information protection certification has been obtained, it is not required to declare a data export security assessment. If personal information of more than 1 million individuals will be provided overseas within ~~one year~~ the next calendar year (excluding the scenarios in Articles 3 and 4), a data export security assessment shall be declared. However, where the personal information is exported overseas based on an individual's consent, consent must still be obtained from the personal information subject; provided that if the data is collected by the Data Processor indirectly from individuals or organizations, the data provider shall be required to obtain the consent of the individuals or organizations in accordance with laws and administrative regulations.*
7	The pilot free trade zone, may on its own, formulate a list of data (hereafter referred to as a	➢ It remains to be clarified as to: - what type of FTZ area will be qualified to	• To the extent possible, relevant regulators to consider providing clarification on the

Cl No.	Content	Comments	Suggestions
	"**Negative List**") that needs to be included within the scope of a data export security assessment, personal information export standard contract, and personal information protection certification management in the pilot free trade zone, and report it to the provincial network security and informatisation commission for approval before submitting it to the national cyberspace administration department for record. For data outside of the Negative List, it is not necessary to declare a data export security assessment, enter into a personal information export standard contract, or obtain a personal information protection certification.	issue the Negative list; - which department in FTZ area will lead the FTZ formulation of the Negative List; - if a PI handler is headquartered in FTZ and has subsidiaries in other cities (non FTZ), will the FTZ policy equally apply to the headquarter and its subsidiaries; and - whether there is a timeline expected for the "Negative List" release. ➢ ~~For those data in the "**Negative List**", is there any change in "Export Mechanism"? considering the current "Export Mechanism" took much longer time than expected, is there any plan to expedite the CAC review process?~~	queries listed in the left column "Comments"
8	Where state organs and the operators of critical information infrastructure provide personal information and important data overseas, it is to be implemented in accordance with relevant laws, administrative regulations, and departmental rules. Where sensitive information involving the Party, government, military, and units involved with secrets or sensitive personal information are provided overseas, it is to be carried out in accordance with relevant laws, administrative regulations, and departmental rules.	➢ Please clarify if the 2nd part of Article 8 applies to provision of sensitive personal information overseas by State Organs and CIIOs and (if yes) recommend the draft regulations to explicitly state so.	• Subject to the actual regulatory intention, CAC to consider whether to revise the second paragraph of this clause with the follow: *"Where State Organs and CIIOs need to provide sensitive information involving the Party, government, military, and units involved with secrets or sensitive personal information overseas ~~are provided~~ overseas, it is to be carried out in accordance with relevant laws, administrative regulations, and*

Cl No.	Content	Comments	Suggestions
			departmental rules."
9	Data handlers providing personal information and important data overseas shall comply with the provisions of laws and administrative regulations, fulfil the obligations of data security protection, and safeguard the security of data outbound. In the event of a data export security incident, or where there is a high security risk in the data export, the data handler shall take remedial measures, and the report the incident to the national cyberspace administration department in a timely manner.	➢ It is unclear as to the scope and determination methods of the "data export security incident" and "high security risk in the data export", which may give rise to implementation issues and compliance uncertainties. ➢ There is a lack of materiality threshold which could lead to over-reporting. Also, it is recommended to consider embodying the relevant reporting requirement into the exiting reporting mechanism that is also relevant to data security issues (e.g., the cybersecurity incident reporting requirement).	• CAC to consider: - providing definitions of the terms and issuing implementation rules (including but not limited to reporting channel and timeline) to facilitate future performance, in particular, it is recommended to include a materiality threshold for the "data export security incident" and "high security risk in the data export" reporting requirement; - giving consideration to the existing incident or risk reporting mechanism relating to data security when setting out the implementation standards and procedures for the "data export security incident" and "high security risk in the data export" reporting requirement to avoid over-reporting, and coordinating with relevant industrial regulators to offer a unified and streamlined reporting system for data security and PI protection issues.
10	The local cyberspace administration departments shall strengthen the guidance and supervision of data processors' data export activities, and strengthen its supervision beforehand, during	➢ The market would expect a consistent and market-friendly regulatory implementation practice after the formal issuance of Draft Provisions,	• CAC to consider carrying out future regulatory implementation in a consistent and balanced method.

	and after the activities. If a higher risk is detected in the data export activities, or if a security incident occurs, the local cyberspace administration department will instruct the data processor to carry out rectification to eliminate hidden dangers; if the data processor refuses to make corrections or if it leads to serious consequences, the data processor will be ordered in accordance with the law to halt data export activities and to safeguard the data security.		
11	Where relevant provisions including the Measures for Data Export Security Assessment and the Measures for Personal Information Export Standard Contract are inconsistent with the Provisions, the Provisions shall prevail.	➢ The current wording is not very clear as to whether the newly provided thresholds will fully replace the application thresholds stipulated under the existing CAC rules such as the *Measures for the Security Assessment of Outbound Data Transfer* and *the Provisions on Standard Contracts for Outbound Transfers of Personal Information*. ➢ The relationship between rules provided under the Draft Provisions and those contemplated/to be issued for the Greater Bay Area (e.g., which rule would prevail) is to be further clarified.	• CAC to consider specifying in the Draft Provisions (i) that (after the formal issuance of the Draft Provisions) the application thresholds stipulated under the existing CAC rules will no longer apply; and (ii) whether the contemplated data transfer rules for the Greater Bay Area will prevail over the Draft Provisions in case of inconsistency.