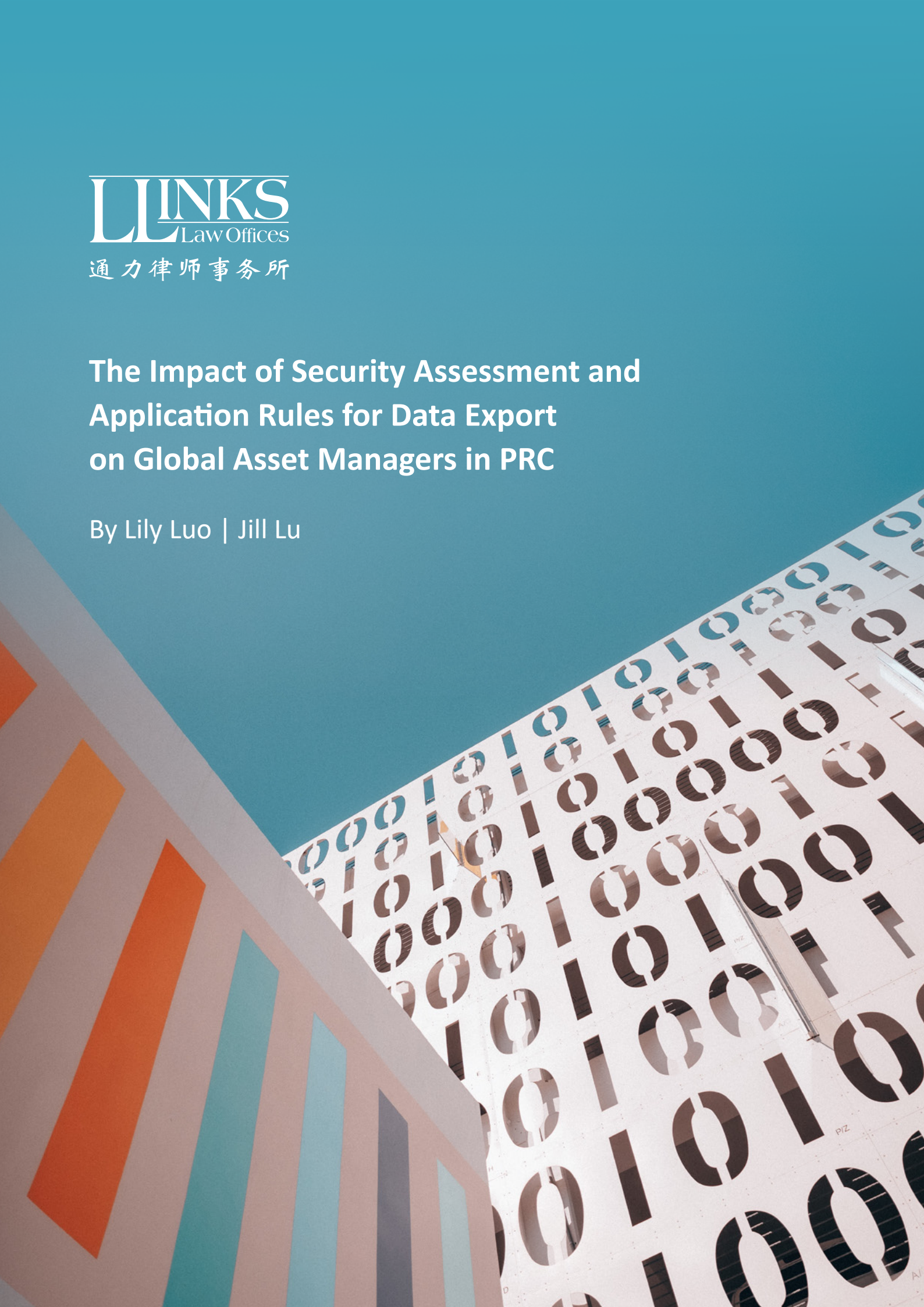
LINKS Law Offices
通力律师事务所

The Impact of Security Assessment and Application Rules for Data Export on Global Asset Managers in PRC

By Lily Luo | Jill Lu



On 31 August 2022, the Cyberspace Administration of China ("**CAC**") promulgated the *Application Guidelines for Data Export Security Assessment (1st Edition)* (数据出境安全评估申报指南(第一版), "**Guidelines**"). The *Guidelines* provides guidance for the implementation of the security assessment of data export ("**Security Assessment**") conducted by the CAC as provided in the *Measures for Data Export Security Assessment* (数据出境安全评估办法, "**Assessment Measures**") issued by the CAC in July 2022, reiterates the scope of application of the Security Assessment, elaborates the methods and procedures for application, and provides the list and templates of the application materials. Both the *Assessment Measures* and the *Guidelines* have come into effect on 1 September 2022.

With the promotion of China's opening up, more and more global asset managers have set up WFOEs or JVs in China to carry out asset management business. Data export is an inevitable need for global asset managers which operate under collectivized management of the group. With the release and refinement of the rules related to the Security Assessment and its application, it is also necessary for global asset managers in PRC to pay attention to the impact of such rules on them.

This article analyzes the impact of the *Assessment Measures* and the *Guidelines* on several types of onshore subsidiaries set up by global asset managers – WFOE PFMs, QDLP entities, WFOE FMCs, WMCs and unregulated WFOEs.

I. Application of the Security Assessment

1. Data Export

On the basis of the CAC's press conference in respect of the *Assessment Measures* in July 2022, the *Guidelines* reiterates and elaborates the meaning of "data export", including:

(1) A data handler transfers or stores abroad the data collected and generated during its operation within the territory of China;

(2) The data collected and generated by a data handler is stored within the territory of China but could be accessed, checked, retrieved, downloaded or exported by offshore institutions, organizations or individuals; and

(3) Any other activity involving data export prescribed by the CAC.

2. Circumstances Triggering the Security Assessment

According to the *Assessment Measures* and the *Guidelines*, not all data export will trigger the Security Assessment. Only the export of critical data and export of personal information under certain circumstances are subject to the Security Assessment.

(1) Definition of critical data

The *Assessment Measures* defines "critical data" as "data that, once tampered with, destroyed, leaked, illegally obtained, or illegally used, may endanger national security, economic operation, social stability, public health, security, etc.". However, the *Information Security Technology – Guideline for Identification of Critical Data* (信息安全技术 重要数据识别指南), which is a national standard, has not been officially promulgated, and there has been no definitive standard for identifying "critical data". T*he Regulations on Cyber Data Security Management (Consultation Paper*) (网络数据安全管理条例(征求意见稿)) issued in November 2021 states the scope of "critical data", which includes "data on safe production or operation in key industries or fields such as finance, and data on component or equipment supply chain of any critical system". However, we tend to believe that this does not mean that all data in the financial industry should be identified as "critical data". The exact definition of critical data is still pending the formal promulgation of the aforementioned regulations and national standard.

Although the national standard for identifying critical data has not yet been officially issued, the *Standardized Practice Guidelines for Cyber Security – Guidelines for the Classification and Grading of Cyber Data* (网络安全标准实践指南——网络数据分类分级指引, "**Classification and Grading Guidelines**") and the industrial standards on data grading issued by the People's Bank of China ("**PBOC**") and the China Securities Regulatory Commission ("**CSRC**") have already been served as reference for identifying critical data by global asset managers in PRC. The relevant correspondence relationship is listed as follows:

	Grading in the industrial standards	Grading in the *Classification and Grading Guidelines*
Financial Data Security – Guidelines for Data Security Classification (金融数据安全 数据安全分级指南)	Level V *	Critical Data
	Level IV	General Data Level IV
	Level III	General Data Level III
	Level II	General Data Level II
	Level I	General Data Level I
Personal Financial Information Protection Technical Specification (个人金融信息保护技术规范)	C3	General Data Level IV
	C2	General Data Level III, Level IV
	C1	General Data Level I, Level II

*In the *Financial Data Security – Guidelines for Data Security Classification* (金融数据安全 数据安全分级指南) issued by the PBOC, the characteristic of data graded as Level V is described

as "critical data, which is generally used for key business of large or extra-large institutions in the financial industry and institutions with important core nodes in the process of financial transactions, is generally made public to specific persons, and is only accessed or used by those who must be aware of the data" and "the breach of data security will have an impact on the national security or serious impact on the rights and interests of the public".

Therefore, prior to the formal promulgation of national standard on the identification of critical data, global asset managers in PRC may refer to the aforementioned standards when determining whether the data export constitutes the cross-border transfer of "critical data".

(2) The export of personal information which triggers the Security Assessment

Under the specific circumstances set forth in the *Assessment Measures*, the export of personal information is subject to the Security Assessment. Such specific circumstances include:

- Critical information infrastructure operators ("**CIIO**") provide personal information abroad;
- A data handler handling personal information of 1 million or more individuals transfers personal information abroad;
- A data handler exporting personal information of over 100 thousand individuals or sensitive personal information of over 10 thousand individuals in aggregate from 1 January of the previous year transfers personal information abroad.

The foregoing also clarifies the circumstances set forth in Article 40 of the *Personal Information Protection Law of the People's Republic of China* (中华人民共和国个人信息保护法, "**PIPL**") where personal information shall only be provided abroad upon completing the Security Assessment.

II. Procedures and Cautions of the Security Assessment

In combination with the *PIPL*, the *Assessment Measures* and the *Guidelines*, if the Security Assessment is triggered, the main application procedures and cautions are as follows:

1. (If the cross-border transfer of personal information is involved) Impact assessment on personal information protection

If the cross-border transfer of personal information is involved, an impact assessment on personal information protection shall be conducted in accordance with Article 56 of the *PIPL*, regardless of whether the Security Assessment is triggered.

2. Preparation of the legal document relating to the data export to be concluded with the offshore recipient ("Proposed Legal Document")

It should be noted that the Proposed Legal Document is one of the application materials for the Security Assessment and should remain unsigned until the Security Assessment is passed. Both the risk self-assessment and the Security Assessment conducted by the CAC on data cross-border transfer shall include an assessment on the contents of the Proposed Legal Document.

Article 38 of the *PIPL* provides four possible routes for cross-border transfer of personal information, i.e. (1) passing the Security Assessment organized by the CAC, (2) obtaining the personal information protection certification by professional institutions, (3) entering into a contract with the offshore recipient in accordance with the standard contract formulated by the CAC ("**Standard Contract**"), or (4) other conditions prescribed by laws and regulations. If the Security Assessment is triggered for the cross-border transfer of personal information, it is a must to choose route (1), and there is no need to sign the Standard Contract. However, on the one hand, Article 9 of the *Assessment Measures* provides the contents of the Proposed Legal Documents, and *the Provisions on Standard Contract for Cross-border Transfer of Personal Information (Consultation Paper)* (个人信息出境标准合同规定(征求意见稿)) also provides that the Proposed Legal Documents should not conflict with the Standard Contract. On the other hand, such Proposed Legal Document should be submitted to the CAC as one of the application materials for the Security Assessment. Therefore, the Proposed Legal Documents shall be reviewed with a relatively strict criteria.

3. Self-assessment on the risk of data export

The *Guidelines* provides a template of the report for self-assessment on the risk of data export, which details the matters in self-assessment as mentioned in the *Assessment Measures*, and requires that the self-assessment shall be completed within three months before applying for the Security Assessment.

4. Application for the Security Assessment

An application for the Security Assessment shall be submitted to provincial departments of the CAC, and the provincial departments of the CAC shall do the completeness check and submit the Security Assessment application to the CAC within 5 working days. The CAC shall decide whether to accept the application and notify the data handler of its decision within 7 working days from the date of receipt of the application materials. Under normal circumstances, the CAC will complete the Security Assessment within 45 working days from the date of issuance of a written acceptance notice.

5. Reassessment

In accordance with Article 14 of the *Assessment Measures*, the Security Assessment result is valid for 2 years commencing from the date of its issuance. If it is necessary to continue carrying out data

export activities after the expiration of the assessment result, the data handler shall re-apply for the Security Assessment 60 working days before the expiration. If any circumstance affecting security of the exported data occurs during the validity period, the Security Assessment shall also be re-applied. Such circumstances include:

(1) Changes in purpose, method, scope, type of data export and changes in offshore recipient's handling purpose and method, which affect the security of the exported data, or extension of offshore storage period of personal information and critical data;

(2) Changes in policies and regulations on data security protection and cyber security environment of the country or region where the offshore recipient domiciles or occurrence of other force majeure events, or changes in the actual control power of the data handler or the offshore recipient, changes in the legal documents entered into by the data handler and the offshore recipient, which affect the security of exported data;

(3) Other circumstances affecting the security of exported data.

For the application and specific procedures of the Security Assessment, please refer to the flow chart attached in the end of this article.

III. Impact of the Security Assessment on Global Asset Managers in PRC

1. Foreign-invested private fund managers (including WFOE PFMs and QDLP entities)

Foreign-invested private fund managers usually operate under collectivized management of the group. They keep close touch with offshore affiliates in sharing business data and information, or leverage the group's global system to handle the data or information collected from onshore. However, we understand that most data of foreign-invested private fund managers will not fall into the category of "critical data".

If, after the issuance of national standard for identification of critical data, the business data of WFOE PFMs and QDLP entities is considered as "critical data", then under the existing business scenarios, WFOE PFMs and QDLP entities will be required to apply for the Security Assessment before they transfer business data to their offshore affiliates. Such business scenarios may include:

(1) Where WFOE PFMs and QDLP entities provide their data of investment and trading, risk control, anti-money laundering, etc. abroad or store such data in offshore, it would constitute data export;

(2) Where WFOE PFMs and QDLP entities store their data of investment and trading, risk control and anti-money laundering, etc. in a system or cloud drive using onshore server, while the

offshore affiliates can access, retrieve, download or export such data, it would also constitute data export in accordance with the *Assessment Measures* and the *Guidelines*.

If the aforementioned data is considered as critical data (though with less possibility), such data could be exported only after completion of the Security Assessment.

In terms of the cross-border transfer of personal information, the following circumstances may be involved:

(1) Where it is necessary, WFOE PFMs and QDLP entities would need to transfer the information of investors abroad or leverage the offshore system of the group for anti-money laundering check. Such investors' personal information includes those of individual investors, relevant individuals of institutional investors and product investors (including legal representatives, handling persons, senior management personnel, beneficial owners, etc. of the institutions or product managers).

In addition, where a QDLP fund invests in an offshore fund, the offshore fund manager will also request the QDLP entity to provide the personal information of relevant individuals of its onshore investors, for the purpose of conducting customer due diligence and anti-money laundering check as well as performing sanctions compliance obligations on investors of the offshore fund.

(2) WFOE PFMs and QDLP entities may transfer the personal information of employees abroad for the purpose of unified personnel management of the group.

(3) It is common that global asset managers require the unified management and due diligence on the service providers and cooperative institutions of the group entities, including anti-money laundering, anti-corruption checks, etc. In such case, the group will request WFOE PFMs and QDLP entities to collect relevant personal information of onshore cooperative institutions such as custodians, outsourcing service providers, distributors and brokers, and transfer such personal information abroad.

(4) The cross-border transfer of personal information also applies if WFOE PFMs and QDLP entities have onshore websites and WeChat official accounts, and collect and transfer abroad the personal information of visitors and subscribers through such websites and WeChat official accounts.

Although it is unclear whether private fund managers will be deemed as CIIOs, according to Article 10 of the *Regulation on the Security Protection of Critical Information Infrastructures* (关键信息基础设施安全保护条例), the CSRC is responsible for the identification of CIIOs in the industry and will

notify the relevant institutions of the result that they are identified as CIIOs. If an institution has not received such notification, it will be inferred that such institution is not deemed as a CIIO.

If WFOE PFMs and QDLP entities are not deemed as CIIOs, the Security Assessment will only be triggered when certain amount of personal information/sensitive personal information is transferred abroad. Given the limit on the number of investors of a private fund, the amount of personal information collected by a WFOE PFM or QDLP entity usually does not meet the threshold of the Security Assessment. However, WFOE PFMs and QDLP entities should also monitor the personal information export based on the accumulative amount of personal information in the past year and in history.

2. **Wholly foreign-owned fund management companies (WFOE FMCs) and joint venture wealth management companies (WMCs)**

The data export of retail fund managers (including WFOE FMCs) is subject to strict restriction. Generally, only the data pre-approved by the CSRC can be transferred abroad. According to Article 66 of the *Measures for the Supervision and Administration of Publicly Offered Securities Investment Fund Managers* (公开募集证券投资基金管理人监督管理办法), without the approval of the CSRC and the relevant competent departments of the State Council, no organization or individual shall provide documents and materials relating to securities business activities to offshore parties. Therefore, the data cross-border transfer of WFOE FMCs shall be subject to prior approval by the CSRC. As far as we know, currently, in the applications for setup of new FMCs and change of shareholding structure of existing FMCs (changing to be foreign-controlled), a prior approval for the white list of data to be transferred abroad might be required. In general, the non-public information (including the investment and research data (with respect to a single issuer or security), product positions and trading information of products launched by FMCs), and non-public operation data such as NAV adjustment data shall not be transferred abroad, nor shall clients' information be transferred abroad.

As to WMCs, in accordance with Article 41 of the *Measures for the Administration of Wealth Management Subsidiaries of Commercial Banks* (商业银行理财子公司管理办法), WMCs shall establish a risk segregation mechanism, and shall not provide its offshore affiliates with key sensitive information related to investment and operation, etc., nor shall it provide materials such as investment, research and clients' sensitive information that may have potential conflict of interests.

For the data that is allowed to be transferred abroad, the basis for determining whether the Security Assessment is required is the same as that described in item 1 above.

To clarify, for licensed institutions such as WFOE PFMs, QDLP entities, WFOE FMCs and WMCs, where they are about to export the non-critical data, even though the Security Assessment is not triggered, they should complete certain prerequisites for such data export in accordance with the current industrial norms and standards for the management of financial data issued by the PBOC.

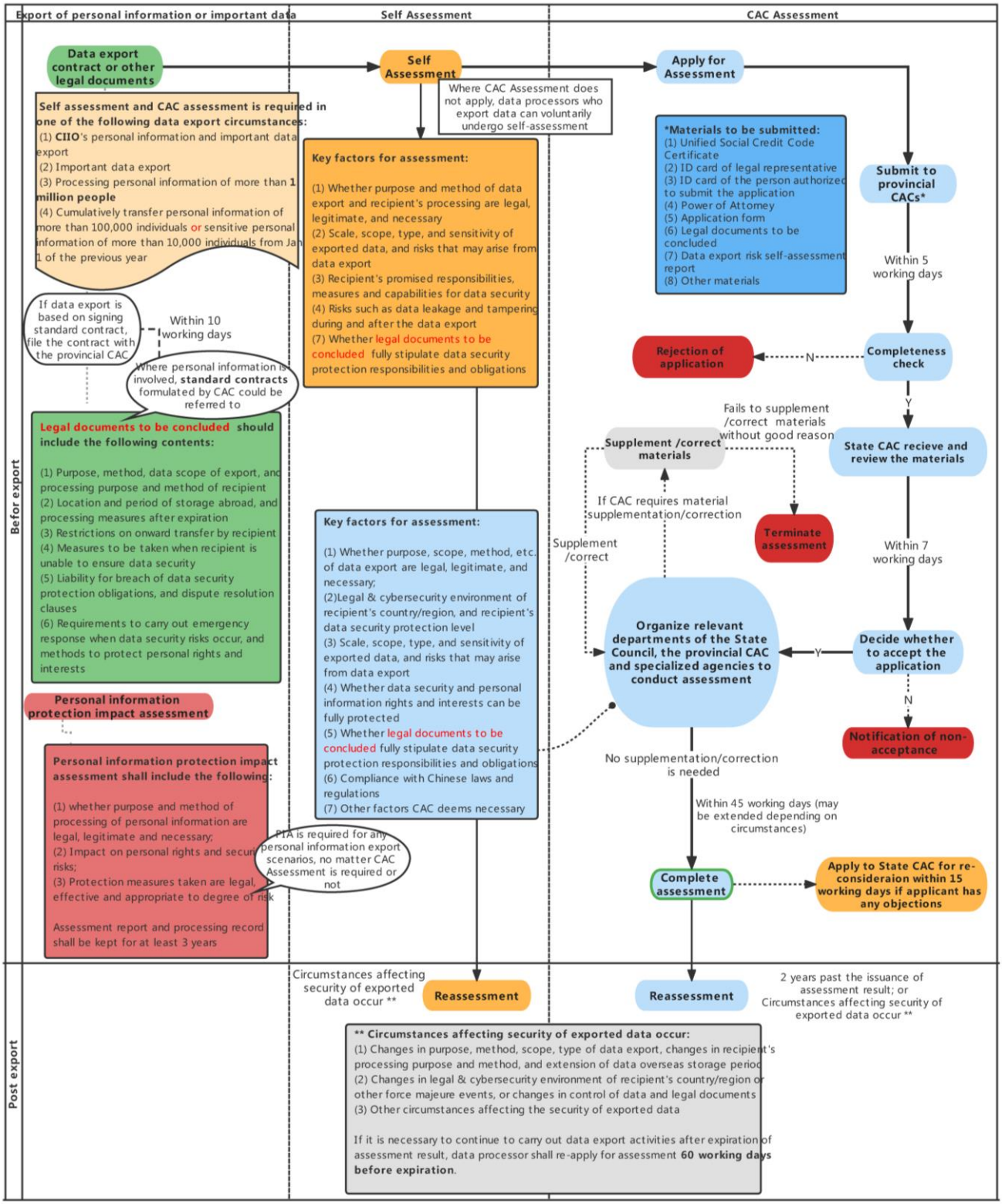
The relevant rules related to financial data issued by the PBOC apply to "financial industry institutions". According to the *Financial Data Security – Guidelines for Data Security Classification* (金融数据安全 数据安全分级指南), "financial industry" includes "monetary and financial services, capital market services, insurance, etc., see GB/T 4754-2017 for details". "Financial industry institutions" refer to "relevant institutions engaging in the above-mentioned financial industry businesses". According to the *Industrial Classification for National Economic Activities* (GB/T 4754-2017) (国民经济行业分类), "financial industry" includes "publicly offered securities investment funds", "non-publicly offered securities investment funds", and "banking financial services", etc.

According to the *Financial Data Security – Security Specification of Data Life Cycle* (金融数据安全 数据生命周期安全规范) which is an industrial standard issued by the PBOC, where a financial data provider provides financial data to an external party, on the one hand, "prior to the data sharing, a data security impact assessment shall be carried out to assess the content, scope, time period, transmission mode, purpose, security management and control measures and other elements of the shared data"; on the other hand, "the provider shall, by signing a contract with the recipient or other means, specify the responsibilities and obligations of both parties with respect to data security and agree on the content, purpose, scope of use and other matters of the shared data". Therefore, with respect to the cross-border transfer of financial data which is not critical data, the provider shall conduct a self-assessment on the impact on data security and enter into a relevant cross-border transfer agreement.

In addition, licensed institutions are also required to pay attention to and implement relevant industrial standards and norms on personal financial information protection and data classification and grading issued by the CSRC, the National Information Security Standardization Technical Committee and the POBC.

Besides, we also note that, for an unregulated WFOE, since it is neither allowed to engage in financial business nor a securities or fund business institution under the CSRC's regulation, the criteria for identifying whether the data of an unregulated WFOE is considered as critical data will be subject to the issuance of the national standard as mentioned above. Given that most unregulated WFOEs engage in group branding, market research and providing client liaison support for the group, we understand that it is very likely that critical data will not be involved.

In addition, an unregulated WFOE will not be expected to be recognized as a CIIO. Considering the nature of the onshore business of an unregulated WFOE, it is unlikely that a large amount of personal information will be transferred abroad. Therefore, the chance that an unregulated WFOE is subject to the Security Assessment is remote. However, unregulated WFOEs shall still pay attention to and monitor the quantity of the exported personal information in combination with specific business scenarios.


Export of personal information or important data
Self Assessment
CAC Assessment
Befor export
Post export
Data export contract or other legal documents
Self Assessment
Apply for Assessment
Where CAC Assessment does not apply, data processors who export data can voluntarily undergo self-assessment
Self assessment and CAC assessment is required in one of the following data export circumstances:
(1) CIIO's personal information and important data export
(2) Important data export
(3) Processing personal information of more than 1 million people
(4) Cumulatively transfer personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals from Jan 1 of the previous year
Key factors for assessment:
(1) Whether purpose and method of data export and recipient's processing are legal, legitimate, and necessary
(2) Scale, scope, type, and sensitivity of exported data, and risks that may arise from data export
(3) Recipient's promised responsibilities, measures and capabilities for data security
(4) Risks such as data leakage and tampering during and after the data export
(7) Whether legal documents to be concluded fully stipulate data security protection responsibilities and obligations
*Materials to be submitted:
(1) Unified Social Credit Code Certificate
(2) ID card of legal representative
(3) ID card of the person authorized to submit the application
(4) Power of Attorney
(5) Application form
(6) Legal documents to be concluded
(7) Data export risk self-assessment report
(8) Other materials
Submit to provincial CACs*
Within 5 working days
If data export is based on signing standard contract, file the contract with the provincial CAC
Within 10 working days
Where personal information is involved, standard contracts formulated by CAC could be referred to
Rejection of application
N
Completeness check
Y
Fails to supplement /correct materials without good reason
Supplement /correct materials
State CAC recieve and review the materials
Legal documents to be concluded should include the following contents:
(1) Purpose, method, data scope of export, and processing purpose and method of recipient
(2) Location and period of storage abroad, and processing measures after expiration
(3) Restrictions on onward transfer by recipient
(4) Measures to be taken when recipient is unable to ensure data security
(5) Liability for breach of data security protection obligations, and dispute resolution clauses
(6) Requirements to carry out emergency response when data security risks occur, and methods to protect personal rights and interests
If CAC requires material supplementation/correction
Terminate assessment
Supplement /correct
Within 7 working days
Key factors for assessment:
(1) Whether purpose, scope, method, etc. of data export are legal, legitimate, and necessary;
(2)Legal & cybersecurity environment of recipient's country/region, and recipient's data security protection level
(3) Scale, scope, type, and sensitivity of exported data, and risks that may arise from data export
(4) Whether data security and personal information rights and interests can be fully protected
(5) Whether legal documents to be concluded fully stipulate data security protection responsibilities and obligations
(6) Compliance with Chinese laws and regulations
(7) Other factors CAC deems necessary
Organize relevant departments of the State Council, the provincial CAC and specialized agencies to conduct assessment
Y
Decide whether to accept the application
N
Notification of non-acceptance
Personal information protection impact assessment
Personal information protection impact assessment shall include the following:
(1) whether purpose and method of processing of personal information are legal, legitimate and necessary;
(2) Impact on personal rights and security risks;
(3) Protection measures taken are legal, effective and appropriate to degree of risk
Assessment report and processing record shall be kept for at least 3 years
PIA is required for any personal information export scenarios, no matter CAC Assessment is required or not
No supplementation/correction is needed
Within 45 working days (may be extended depending on circumstances)
Complete assessment
Apply to State CAC for re-consideraion within 15 working days if applicant has any objections
Circumstances affecting security of exported data occur **
Reassessment
Reassessment
2 years past the issuance of assessment result; or Circumstances affecting security of exported data occur **
** Circumstances affecting security of exported data occur:
(1) Changes in purpose, method, scope, type of data export, changes in recipient's processing purpose and method, and extension of data overseas storage period
(2) Changes in legal & cybersecurity environment of recipient's country/region or other force majeure events, or changes in control of data and legal documents
(3) Other circumstances affecting the security of exported data
If it is necessary to continue to carry out data export activities after expiration of assessment result, data processor shall re-apply for assessment 60 working days before expiration.

If you would like to know more information about the subjects covered in this publication, please contact:

Lily Luo
+86 21 3135 8732
lily.luo@llinkslaw.com

Jill Lu
+86 21 3135 8729
jill.lu@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD