The Dust Has Settled: Measures for Security Assessment of Data Exports

By David Pan | Nigel Zhu | Susan Deng | Shana Sha

2022 年 7 月 7 日，《数据出境安全评估办法》正式发布，9 月 1 日起施行，从征求意见稿到正式发布，历时仅 8 个月。《评估办法》为企业实施《网络安全法》《个人信息保护法》以及《数据安全法》规定的数据出境安全评估提供指引。通力数据合规团队对最新出台的《评估办法》推出重磅双语法评，中文版请见【尘埃落定！一文详解《数据跨境传输安全评估》重点规定】。

The "2021 Data Economy Report" released by the United Nations revealed that the United States and China benefit greatly from the digital economy. Half of the world's ultra-large-scale data centers are in China and the United States. Global digital companies derive strong financial, market and technical strength from worldwide platform businesses. Considering the presence of a variety of business scenarios such as global supply chain, overseas remote operation and maintenance, cross -border service platform operations, and overseas brand management, the compliance issues involved in data cross-border flow increasingly draw concern. In 2021, we made concise illustration on the data outbound rules under Chinese Law, including security assessment process, in the "Illustrative Chart - Data Outbound Rules".

With the newly published regulation, we have refined the Illustrative Chart to include the newly-established assessment requirements and personal information export rules, please see [双语图解!一图读懂数据出境规则].

For more Llinks publications, please contact:

Publication@llinkslaw.com

Highlights:

The Cyberspace Administration of China ('CAC') issued, on 7 July 2022, the Measures for Security Assessment of Data Exports ("Assessment Measures"), which will take effect on 1 September. It took only 8 months from its exposure draft to formal draft. We conclude highlights of the Assessment Measures as follows:

(1) Conditions triggering CAC assessment stipulated in the exposure draft remain unchanged;
(2) The maximum time period for calculating "individuals accumulated" is two years;
(3) Further refine the procedures and requirements for self-assessment, CAC assessment, and re-assessment;
(4) Expand the document type from "data export contract" to "data export legal documents";
(5) Provide formal definition of "important data";
(6) For any non-compliance in current data export activities, rectification according to the Assessment Measures shall be completed before 1 March, 2023 (within 6 months upon the effective date of the Assessment Measures).

The Assessment Measures provides detailed guidance for companies to conduct data export related assessments stipulated in the *Cybersecurity Law* ("CSL"), *Personal Information Protection Law* ("PIPL") and the *Data Security Law* ("DSL"). This article will interpret the highlights of the latest Assessment Measures and provide compliance suggestions for enterprises to implement data export security assessment.

Main Content:

- Briefing on Assessment Measures and legislative history
- Application scope of data export security assessment
- Data export assessment requirements for specific industries
- Supporting regulations and national standards for data export assessment
- Procedures of data export security assessment (self-assessment, CAC assessment, data export documents, PIA)
- Compliance suggestions

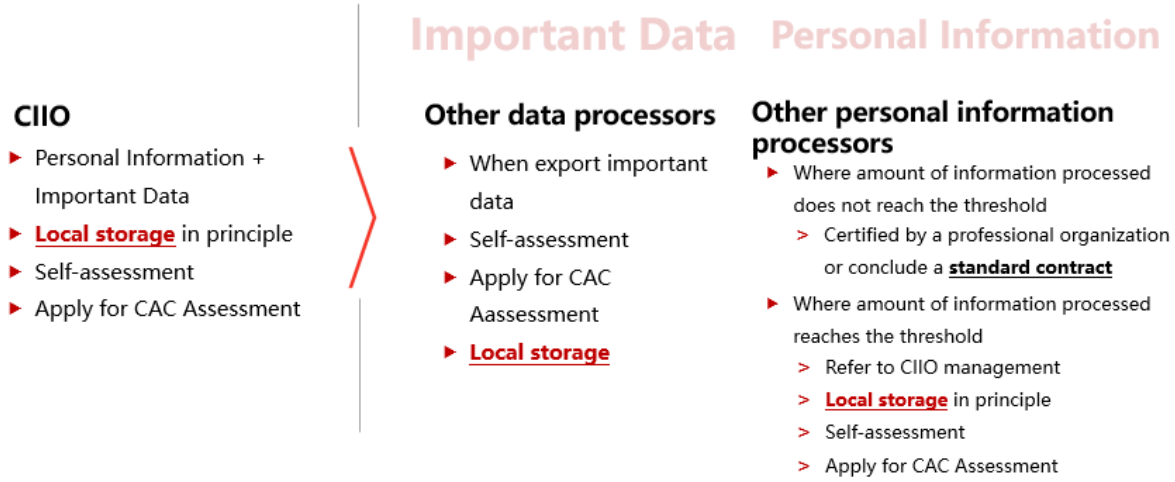
1. Briefing on Assessment Measures

The Assessment Measures is the supporting implementation rules of its upper laws of the CSL, DSL and the PIPL.

In 2017, the CSL, regulated data export activities for the first time, requiring CIIOs to locally store personal information and important data collected in China. Prior to data export due to business needs, security assessment should be conducted in accordance with the law. Since then, the DSL and PIPL set forth different security assessment requirements for important data and personal information. The Assessment Measures clarifies the objects and subjects of the data export security assessment according to the above-mentioned laws:

	Subjects of the assessment	Objects of the assessment
CSL	CIIO	Personal information + important data
DSL	CIIO + other data processors	Important data
PIPL	CIIO+ special personal information processors	Personal information
Assessment Measures	Data processors(CIIO + others)	Personal information + important data

2. Application scope of Data Export Security Assessment



For CIIOs' data export, the Assessment Measures is consistent with the provisions of the CSL, i.e., CIIOs should conduct the security assessment for export of important data and personal information, and the amount of personal information processed by CIIOs is not the criterion for determining whether security assessment is required.

For non-CIIOs, according to the Assessment Measures, security assessment must be conducted in four cases:

(1) When important data is exported;

(2) When personal information processor, which processes personal information of more than 1 million individuals, exports personal information;

(3) When a data processor accumulatively exported personal information of more than 100,000 individuals since January 1 of the preceding year;

(4) When a data processor accumulatively exported sensitive personal information of more than 10,000 individuals since January 1 of the preceding year.

The Assessment Measures clarifies the "threshold prescribed by the CAC" stipulated in the PIPL, i.e., a personal information processor that processes personal information of 1 million people should conduct the security assessment when exporting personal information. This also suggests that the amount of personal information determines whether a security assessment is needed. Since enterprises controlling large amount of personal information face severe data security risks and data compliance obligations, it is

reasonable to classify personal information processors in terms of the amount of personal information processed. According to the Assessment Measures, if an enterprise with a large amount of personal information does not constitute a CIIO, and only exports a relatively small amount of personal information, it is still required to conduct the data export security assessment, which may increase the compliance burden. However, in this scenario, the risk of the enterprise's data export is low, and the enterprise could fully explain the scenarios in the self-assessment report and other documents, so as to pass the security assessment as soon as possible.

With regard to the threshold for triggering data personal information export security assessment, as we mentioned in our article "Highlight of Draft Personal Information Export Standard Contract", Article 4 of the *Personal Information Export Standard Contract (Exposure Draft)* stipulates that the number of data to be exported is to be calculated from January 1 of the preceding year. This provision narrows down the time range for calculating the number of individuals involved in data export, and may impose difficulties for enterprises to apply data export rules. However, the formal Assessment Measures has adopted the same rolling calculation principle, which effectively solves the above contradiction. As a result, for all non-CIIOs and personal information processors that process personal information of less than 1 million individuals, the cumulative calculation of export data will be applied on a rolling basis to determine which data export compliance path is applicable. For example, suppose an MNC uses global systems to export personal information, as long as the number of personal information subjects is below the prescribed threshold for two consecutive calendar years, there is no need to apply for the security assessment.

3. Data Export Assessment Requirements for Specific Industries

In addition to the Assessment Measures, some industry authorities have issued laws and regulations related to data export security assessment applicable to those industries. Enterprises should, based on the provisions of Assessment Measures, follow the laws and regulations effective in the respective industry.

Take automotive data and industrial data as an example, the *Several Provisions on Automotive Data Security Management (for Trial Implementation)*, which came into effect on October 1, 2021, requires that risk assessment should be conducted when transferring automotive data (which constitute important data[1]) abroad. It also requires that automotive data processors should not transfer data abroad beyond the purpose, scope, method, data type and scale specified in the export security assessment. In February 2022, the second draft of *Data Security Management Measures in the Field of Industry and Information Technology (for Trial Implementation)* requires that when it is necessary for data processors in the field of industry and information technology to transfer important data and core data abroad, they should conduct an data export

(I) geographic information, passenger flow, vehicle flow and other data of important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and Party and government organs at the county level or above;
(II) data reflecting economic operation such as vehicle flow, logistics, etc.;
(III) operational data of the automobile charging network;
(IV) video and image data outside the vehicles that contain face information, license plate information, etc.;
(V) the personal information of more than 100,000 persons as the subjects of personal information is involved.

security assessment. Since core data causes greater concerns, enterprises should establish appropriate policies, management and technical measures for the export of core data.

Moreover, some industry authorities usually require specific types of data not to be stored in overseas servers, such as population health data, map data, human genetic resources information, etc. Enterprises in such industries should be cautious with relevant data export activities.

4. Supporting Assessment Regulations and National Standards for Data Export

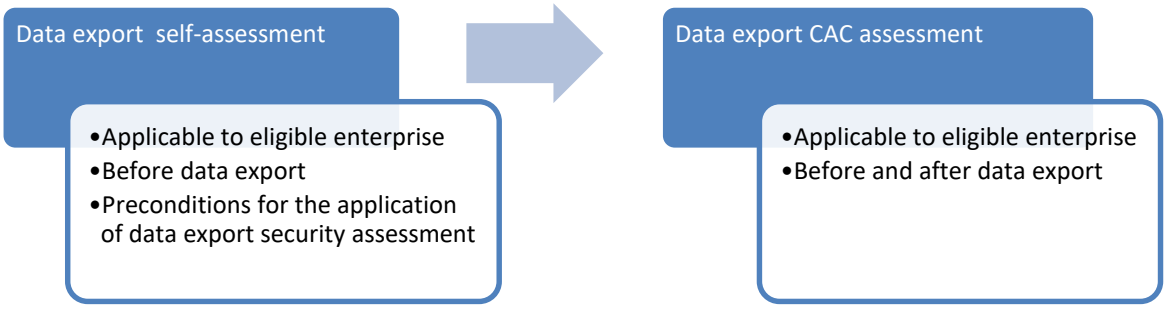
The national standard *Information Security Technology Guidelines for Data Export Security Assessment (Exposure Draft)* provides more detailed regulations on data export activities, such as the definition of data export and the identification of important data. It guides data export assessment processes. Since the national standard is still an exposure draft, enterprises should generally follow the provisions of the Assessment Measures when conducting the assessment, and could refer to the national standard for those cases where the *Assessment Measures* is unclear or not specified.

It is worth mentioning that, prior to the promulgation of the Assessment Measures, the *2017 Measures for the Security Assessment of Personal Information and Important Data Export (Exposure Draft)* and the *2019 Measures for the Security Assessment of Personal Information Export (Exposure Draft)* respectively regulated data export activities. The 2017 Regulation requires all network operators to assess the export of both personal information and important data, while the 2019 Regulation only regulates the export of personal information of network operators. In comparison, following the provisions of the CSL, DSL, and the PIPL, the Assessment Measures provided a clearer assessment process, and substantially replaces the 2017 and 2019 regulations.

5. Content of Data Export Security Assessment

(1) Self-assessment and Security assessment

The Assessment Measures requires both "prior assessment and on-going supervision" and "self-assessment and security assessment". The self-assessment and security assessment ("CAC Assessment") stipulated in the Assessment Measures run through the whole process from pre-data export to post-data export:



In terms of the content of the assessment, there are some overlaps between self-assessment and CAC Assessment. Meanwhile, the two types of assessments have their own focuses, which mainly include the following aspects:

Content of assessment	**Data export self-assessment**	**Data export CAC Assessment**
Data export activities	(I) The legality, legitimacy and necessity of the purpose, scope and method of data export	(I) The legality, legitimacy and necessity of the purpose, scope and method of data export
The circumstance of the export data and the protection of individual rights	(II) The scale, scope, type and sensitivity of export data, and the risk of data export on national security, public interests, and the legitimate rights and interests of individuals or organizations (IV) The risk of data being tampered, destroyed, leaked, lost, transferred or illegally obtained or illegally used during and after export, and whether the channels for protecting the rights and interests of personal information are smooth	(III) The scale, scope, type and sensitivity of the export data, and the risk of data being tampered, destroyed, leaked, lost, transferred or illegally obtained or illegally used during and after export (IV) Whether data security and the rights and interests of personal information can be fully and effectively protected
Related provisions on foreign recipient	(I) The legality, legitimacy and necessity of the purpose, scope and method of the processing of the data by the foreign recipient (III) The duties and obligations which the foreign recipient commits to perform, and whether the foreign recipient's organizational and technical measures and capabilities in terms of performing the duties and obligations can guarantee the security of the export data	(II) The impact of the data security protection policies and regulations as well as cybersecurity environment of the country or region where the foreign recipient is located, and the effect thereof on the security of the export data. Whether the data protection level of the foreign recipient meets the requirements under the laws, regulations and mandatory national standards of the PRC
Data export documents	(V) Whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts, or other legal documents to be concluded with the foreign recipient	(V) Whether the responsibilities and obligations for data security protection are fully agreed in relevant legal documents

Legitimacy	/	(VI) Whether the recipient complies with the laws, regulations and department rules of the PRC
Other matters	(VI) Other matters that may affect the security of data export	(VII) Other matters that the CAC considers necessary to assess

(2) Data Export Documents

No matter to complete the self-assessment or the CAC Assessment, the two types of assessments both assess whether the related data export legal documents (hereinafter referred to as "Data Export Documents") are effective and sufficient. We also pointed out in the Highlight of Draft Personal Information Export Standard Contract that no matter how enterprises transfer data abroad, they should sign data export agreements with foreign recipients.

The Assessment Measures requires enterprises to fully agree on the responsibilities and obligations of data security protection with the recipients in the export documents. Specifically, the Data Export Documents should at least include the following contents:

(a) The purpose, method of data export and the type of export data;
(b) The type, purpose, and method of data processed by the foreign recipient;
(c) The storage method and retention period of export data, and the measures taken by the recipient after the expiration of the retention period or when the processing purpose is satisfied;
(d) The requirements for the re-transfer of export data;
(e) Data security measures which should be taken when data security is difficult to guarantee due to changes of the data recipient or the data security environment in which the recipient is located;
(f) Remedies, liabilities and dispute resolutions for breach of data security obligations;
(g) Channels and methods to properly respond individual's requests, and to safeguard individuals' personal information rights when export data faces security risks.

In addition, according to the PIPL, enterprises need to meet one of the four basic conditions to export data for business purposes. Where there is no need to apply for mandatory security assessment, the most convenient and compliant way for enterprises to transfer data abroad is to sign a standard contract formulated by the cyberspace department. At present, enterprises can refer to the provisions of the *Personal Information Export Standard Contract (Exposure Draft)* and make corresponding modifications and improvements to the current data export documents.

(3) The personal information protection impact assessment and the security assessment

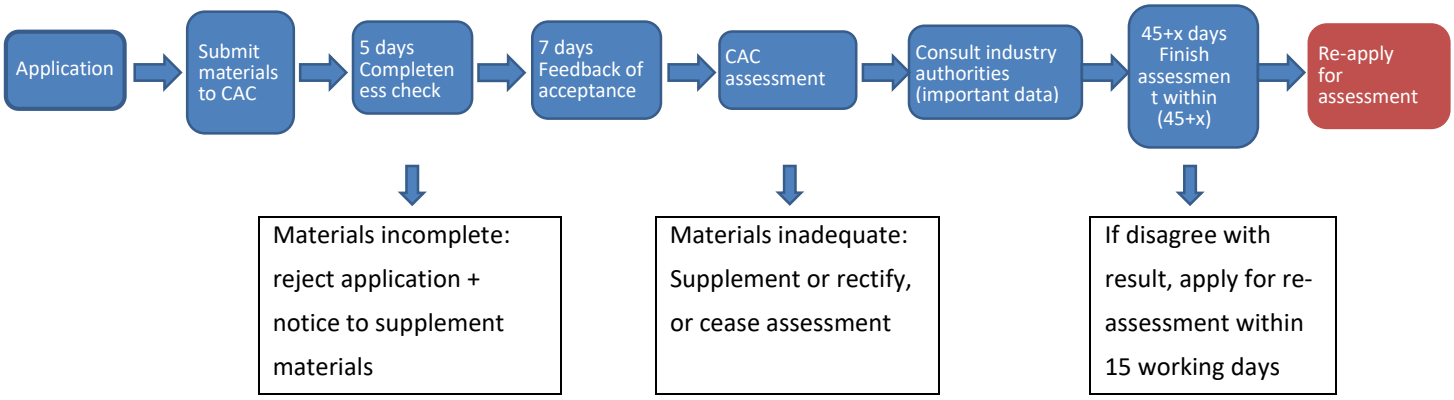
It should be noted that the PIPL requires enterprises to conduct personal information protection impact assessment ("PIA") before providing personal information abroad. PIA should assess the legality and necessity of processing, the impact on and the risks of personal rights and interests, and the

legality and effectiveness of security measures. These assessment requirements are also included in the self-assessment and the CAC Assessment stipulated in the Assessment Measures. Therefore, as a prior assessment, enterprises can sort out the data export scenarios, and combine PIA with data export security assessment.

6. The Procedures of Data Export Security Assessment

(1) Application and review process

According to the Assessment Measures, the steps of applying for the security assessment are as follows.



(2) Re-apply for security assessment

In the following scenarios, enterprises need to re-apply for security assessment:

(a) Expiration of the validity period: the two-year validity period of the data export assessment result expires; or

(b) Processing circumstances change, which no longer meet the data export security management requirements.

In the exposure draft of the Assessment Measures, changes in processing circumstances were specified in detail, which are replaced in the formal version with generalized descriptions. Data processors can still refer to previous provisions in the exposure draft to determine what constitutes “changes in processing circumstances” and thus determine whether the data export security requirements are met.

7. Compliance Suggestions

(1) For the export of personal information and sensitive personal information, enterprises should pay attention to the "accumulative" threshold proposed by the Assessment Measures. Because companies could easily meet such threshold, companies should prepare for CAC assessment when the number of individuals accumulated becomes close to the threshold.

(2) The Assessment Measures clearly determines the application scope of security assessment data, from the perspective of nature and quantity. As far as the identification of important data is concerned, since only industry authorities in financial, automobiles and industry and information sectors have provided important data identification guidelines at the moment, companies should still pay close attention to the data types that may constitute important data, and prepare for the security assessment.

(3) Because the control points and procedures of self -assessment highly coincide with those of the CAC assessment, companies could establish a consolidated solution to complete the two procedures with relatively low cost.

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

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com

Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

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

SHENZHEN

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

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

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