The Dior Case:
Decoding China's New Data Export Enforcement Landscape

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

On September 9, 2025, Chinese police fined fashion giant Dior's Shanghai subsidiary because the company illegally transmitted data overseas without security screening, failed to obtain separate consent and to adopt appropriate security measures. It is a landmark case after China's data export regulatory framework finally established. In this article, we will navigate you through China's cross-border data transfer mechanisms.

China's data export regulatory framework is shaped by the country's Cybersecurity Law ("**CSL**"), Data Security Law ("**DSL**"), and Personal Information Protection Law ("**PIPL**"), which set forth three routes for data export that meet the prescribed thresholds: (i) data export security assessment (the "**Security Assessment**"); (ii) personal information export standard contract clauses (the "**SCC Filing**"); and (iii) personal information protection certification (the "**Certification**"). In this article, the obligations mentioned (i) through (iii) are collectively referred to as "**Data Export Approvals**".

The three data export routes are further supplemented by the following regulations issued by the CAC:

1) Data Export Security Assessment Measures (the "**Security Assessment Measures**"): effective from September 1, 2022;
2) Announcement re Implementation of Personal Information Protection Certification (the **"Protection Certification Measures**"): effective from November 4, 2022; and Measures for Personal Information Protection Certification for Personal Information Export (Exposure Draft) (the **"Export Certification Measures"**): announced on January 3, 2025:
3) Personal Information Export Standard Contract Clauses Measures (the "**SCC Measures**"): effective from June 1, 2023;
4) Facilitation and Regulation of Data Cross-border Transfer Measures (the "**Data Export Measures**"): effective from March 22, 2024.

For more Llinks publications, please contact:

Publication@llinkslaw.com

With the CSL, DSL, PIPL and the above supplementary rules, China now has a well-established data export regulatory framework, mainly regulating the export of personal information and important data.

Key points:

(1) China's data export regulatory framework generally regulates the export of only important data and personal information, and other types of data can be freely exported (note that industrial regulators may issue special rules to regulate the export of special types of data in certain business sectors);

(2) Particularly, if the PIPL applies to a personal data controller located out of China, the personal information collection thereof will be deemed as "personal information export". Thus, such controllers need to examine whether SCC Filing or Certification is needed.

(3) The Security Assessment applies to the export of personal information and important data; whereas the SCC Filing and the Certification apply to only personal information;

(4) Most **personal information** export activities can be exempted from the Data Export Approvals if such export (i) is necessary for the conclusion or fulfilment of contract to which the data subject is a party; or (ii) is necessary for an entity's cross-border human resources management, and is carried out according to lawfully established collective employment agreements or internal human resources policies; or (iii) is necessary for the protection of human or property safety in an emergency; or (iv) does not involve the export of personal information of more than 100,000 (excluding sensitive personal information) people since January 1 of a given year (the above exemptions are referred to as "**Block Exemptions**" in this article);

(5) A Security Assessment is required: (i) where any entity exports important data; (ii) where a Critical Information Infrastructure Operator ("**CIIO**") exports important data or personal information; (iii) where the Block Exemptions do not apply, and an entity exports personal information of more than one million people, or sensitive personal information of more than ten thousand people since January 1 of a given year;

(6) A SCC Filing or a Certification is required where the Block Exemptions do not apply, and an entity exports personal information of over 100,000 people, or any sensitive personal information since January 1 of a given year;

(7) Free Trade Zones ("**FTZ**") within China can and have issued general data export inventories to regulate data export activities within the FTZs.

(8) Data that does not fall into the scope of the Data Export Approvals can be freely exported.

Main Contents:

1. Evolvement of China's Data Export Regulatory Framework

In 2017, CSL came into effect. The CSL is the first legislation to regulate data export activities, 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.

The PIPL came into force in 2021, and it sets forth the regulatory framework for the export of personal information.

Effective in 2022, the Security Assessment Measures require that CIIOs and non-CIIOs which meet the thresholds prescribed in the Security Assessment Measures must file for and complete Security Assessments before they can export important data and personal information.

In 2022 and 2023, the Protection Certification Measures and the SCC Measures came into effect respectively. These two regulations basically require any entity that exports any personal information to file for and complete a SCC Filing or Certification. The detailed rules for personal information export certification measures, i.e., the Export Certification Measures was announced to seek public opinions on January 3, 2025. The Export Certification Measures provides that if the PIPL applies to a personal data controller located out of China, the personal information collection thereof will be deemed as "personal information export".

In March 2024, the Data Export Measures came into effect. The Data Export Measures significantly amends the legal framework established under the Security Assessment Measures, the Protection Certification Measures and the SCC Measures, providing for the Block Exemptions to alleviate the burden on a large number of entities to obtain the Data Export Approvals.

Accordingly, a thorough understanding of China's current data export regulatory framework requires a comprehensive reading of all the regulations above, bearing in mind that the Data Export Measures trump any contradictory requirements in previous legislations.

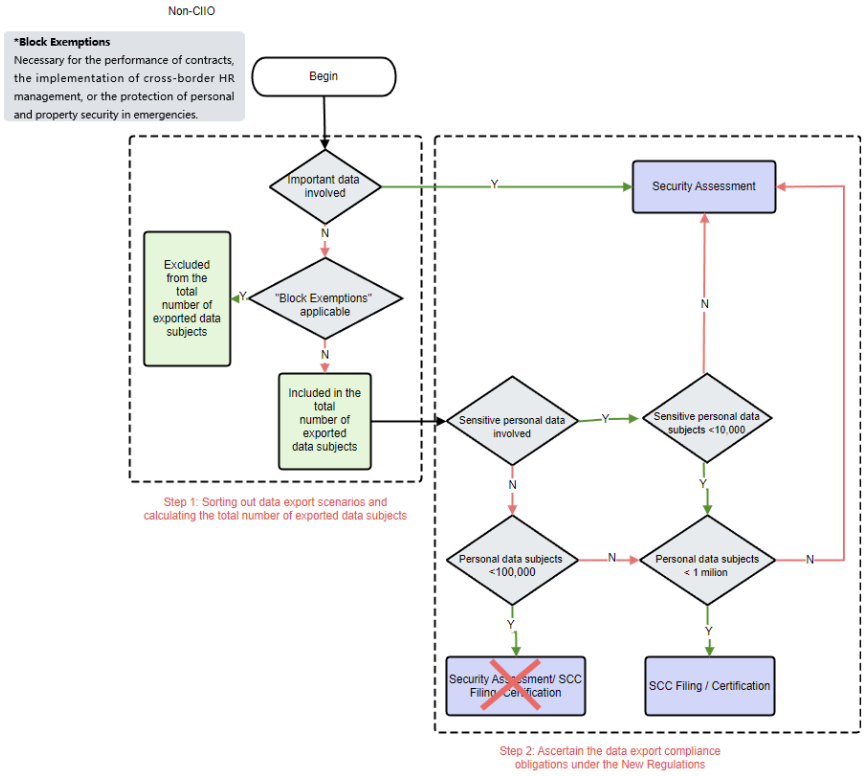
Under China's current data export regulatory framework, different types of data exporters regulated and the types of data regulated is summarized as follows:

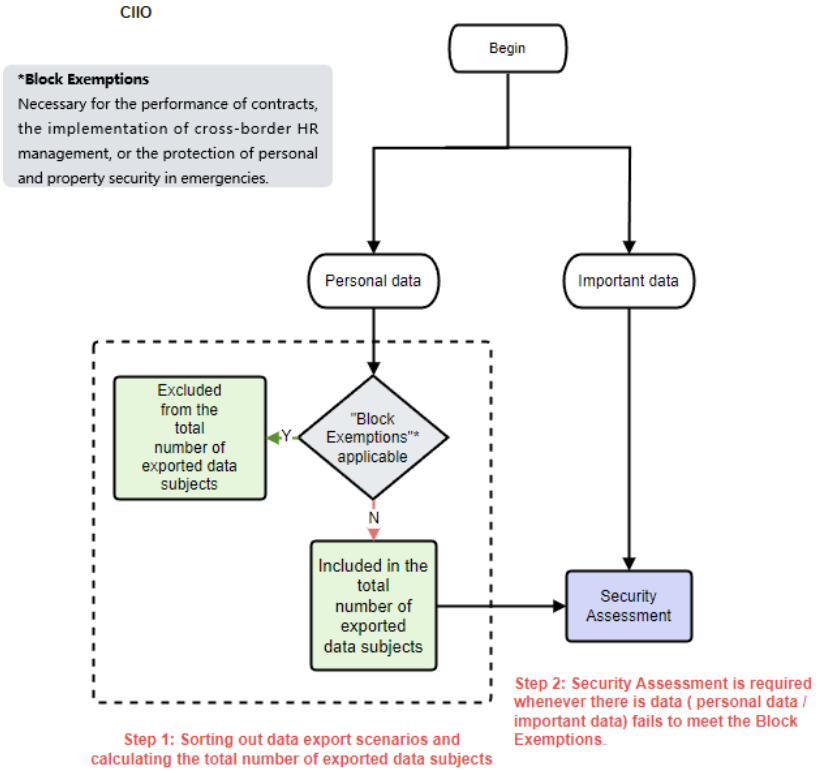
	Types of data exporters regulated	**Types of data regulated**
CSL	CIIOs	Personal information + important data
DSL	All data controllers	Important data
PIPL	CIIOs + personal data controllers meeting relevant thresholds	Personal information
Security Assessment Measures	All data controllers	Personal information + important data
SCC Measures,	Personal data controllers meeting relevant thresholds	Personal information

Protection Certification Measures and Export Certification Measures		
Data Export Measures	CIIOs + personal data controllers meeting relevant thresholds	Personal information + important data

2. Application of the Data Export Approvals

Before diving into details, below we prepare two flowcharts (for CIIOs and non-CIIOs respectively) for data exporters' easy reference in determining whether they need a Data Export Approval and which one to apply for:





2.1. The Block Exemptions and free flow of data

As mentioned above, the most significant change made by the Data Export Measures to the previous data export regulatory framework is the introduction of the Block Exemptions. As the word "Facilitation" in the title of the Data Export Measures suggests, the regulation aims to facilitate the free flow of data by introducing the Block Exemptions.

Specifically, the Block Exemptions mean that in the following circumstances, a data exporter that otherwise is subject to the Data Export Approvals is exempted from such obligations and can freely export the personal information it intends to export:

1) where it is necessary to export personal information for the purpose of concluding or performing a contract to which a data subject is a party, such as cross-border E-commerce, cross-border shipping, cross-border wire transfer, cross-border payment, cross-border account opening, air ticket and hotel reservation, visa processing and examination services;
2) where it is necessary to export employees' personal information for the purpose of conducting cross-border human resources management in accordance with internal corporate policies and regulations formulated in accordance with law, and collective contracts concluded in accordance with law;
3) where it is necessary to export personal information in an emergency to protect the life, health and property safety of a natural person; or
4) where a non-CIIO data controller exports the personal information (excluding sensitive personal information) of not more than 100,000 persons accumulatively since January 1 of the given year.

(Please note that the Block Exemptions only apply to the export of personal information)

Therefore, for data exporters in China, the first step to determine whether they need to obtain a Data Export Approval is to determine whether any of the Block Exemptions apply to them. In a specific data export scenario (such as the export of employees' personal information, the export of consumers' personal information), if the answer is yes, then the data exporter is free to export its personal information. However, if there are any data export scenarios where none of the Block Exemptions apply, then the data exporter needs to determine which one of the Data Export Approvals it needs to apply for and obtain.

2.2. The Security Assessment

The Security Assessment applies to the export of both personal information and important data.

2.2.1. Personal information

In terms of personal information, as mentioned above, the Security Assessment is only applicable where the Block Exemptions do not apply.

Where the Block Exemptions do not apply, the Security Assessment will be triggered if: (i) a CIIO exports any personal information; or (ii) a data exporter exports personal information of more than one million people, or sensitive personal information of more than ten thousand people since January 1 of a given year.

2.2.2. Important data

Block Exemptions do not apply to export of important data. Any data exporter that exports important data, regardless of the data's amount or the purpose of the export, and regardless of the data exporter's status as a CIIO or non-CIIO, must apply for and go through the Security Assessment.

Please note that personal information in certain special forms may constitute important data under PRC law (for example, in the automotive industry, the combination of personal information of more than 100,000 persons is deemed important data), and the Block Exemptions cannot be applied to the export of such personal information and a Security Assessment must be applied for.

2.3. The SCC Filing/Certification

The SCC Filing or the Certification only applies to the export of personal information.

Where the Block Exemptions do not apply, the SCC Filing/Certification will be triggered if a data exporter exports personal information of more than 100,000 people (but less than one million people), or any sensitive personal information since January 1 of a given year.

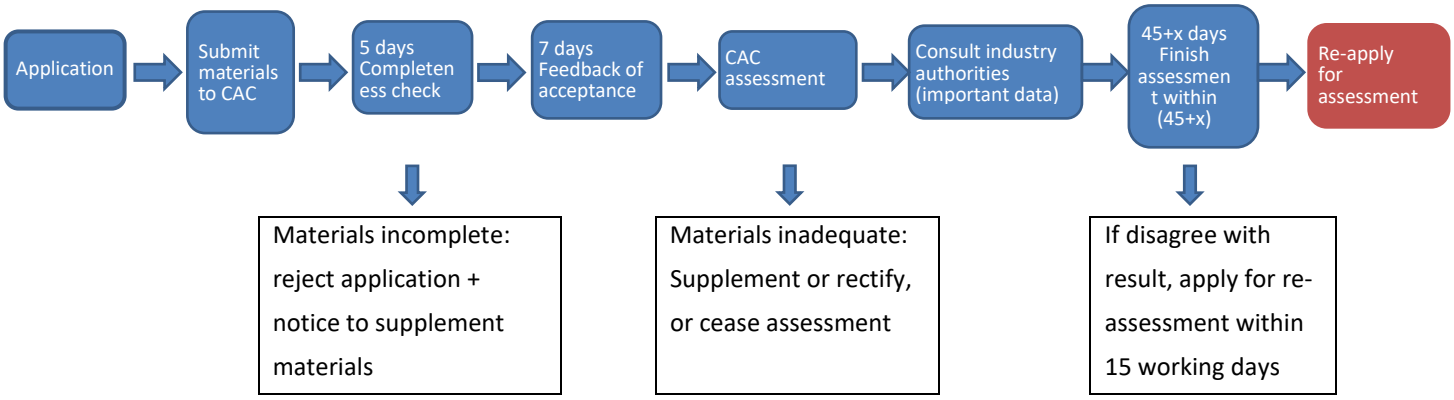
If a personal data controller located out of China needs to go through Certification, the application should be made by its specialized agency or its designated representative in China.

3. The Procedures of Obtaining Data Export Approvals

3.1. The Security Assessment

(1) Application and review process

According to the Security Assessment Measures, the procedures of completing a Security Assessment are as follows:



(2) Re-application

In the following scenarios, data exporters that have obtained an approval for the Security Assessment need to apply for the extension of a Security Assessment approval or need to make a re-application:

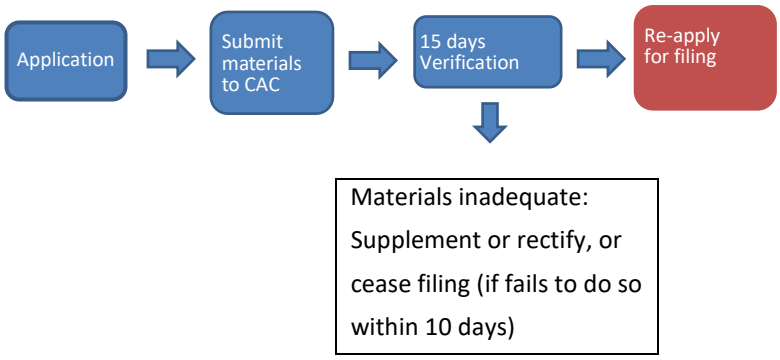
(a) Expiration of the validity period: the approval for a Security Assessment is valid for three years. If the circumstances of data export have not changed during the three-year period, data exporters may apply to the CAC 60 days before the expiration date to extend the validity of the Security Assessment approval for another three years; or

(b) Changes in data export circumstances: whenever the circumstances of a data exporter's data export activities change, so that the information filed with the CAC in the Security Assessment no longer reflects the facts of the data exporter's data export activities, the data export must re-apply to the CAC for a Security Assessment.

3.2. The SCC Filing

(1) Application and review process

According to the SCC Measures, the procedures of completing an SCC Filing are as follows:



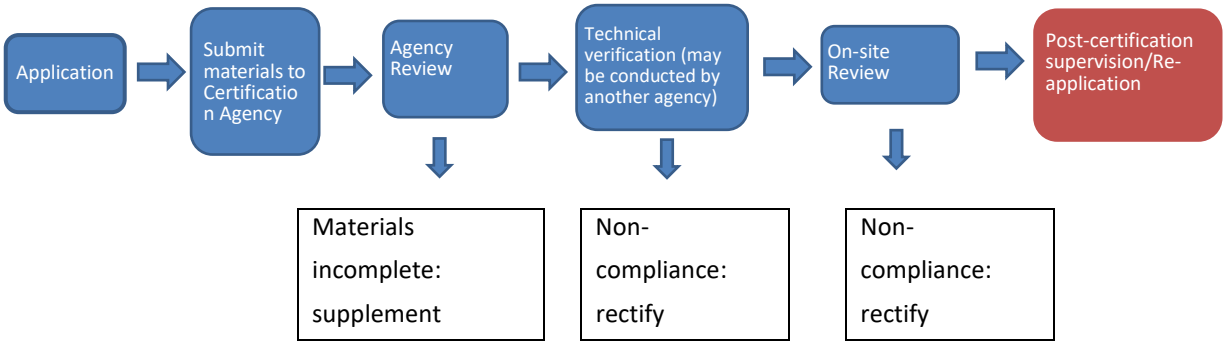
(2) Re-application

Unlike the Security Assessment, the result of an SCC Filing is valid as long as the SCC remains effective. Only when circumstances of a data exporter's data export activities change will the data exporter be obligated to apply to the CAC to update its original SCC Filing.

3.3. The Certification

(1) Application and review process

Certification should be carried out by professional certification agencies that have obtained the qualifications for personal information protection certification ("**Certification Agency(-ies)**"). Such Certification Agencies should go through the filing formalities with the CAC. The procedures of completing a Certification are as follows:



(2) Post-certification supervision/Re-application

Once completed, the Certification is valid for 3 years. Throughout the validity period, the Certification Agency and the CAC will conduct ongoing supervision to ensure that the data

exporter continuously complies with the Certification requirements, and has the right to suspend or revoke the Certification if the data exporter no longer meets the requirements. The data exporter may apply for renewal six months before the expiration date of the Certification.

When circumstances change (such as the entity's name, registered address, Certification requirements, Certification scope), the data exporter is obliged to apply to the Certification Agency to update its original Certification. The Certification Agency will then review the new application materials and may re-conduct technical verification and/or on-site review as deemed necessary.

4. Data export inventories

Another key aspect of China's data export regulation is the government's issuance of data export inventories by FTZs across China. These data export inventories generally aim to ease restrictions on data export activities that take place within the FTZs.

Data export inventories may take the form of negative lists or positive lists. A negative list provides for data types that are prohibited from export or need to complete the above data export compliance requirements, and all data beyond the scope of the negative list may be exported freely. On the contrary, a positive list provides for data that can be freely exported, and data types not on the list need to fulfill the obligations such as completing the Security Assessment or the SCC filing as required by the Data Export Measures or other relevant China's laws and regulations.

The most notable development in this regard is the negative list published by the Tianjin FTZ, and the positive list published by the Shanghai Lin-gang FTZ.

The Lin-gang Positive List contains a number of data types that can freely flow out of China subject to certain undertakings and technical protection measures by data exporters. As an example, the part relating to intelligent connected vehicle data in the Lin-gang Positive List looks like the follows:

No.	Applicable Subject	Data Export Scenario	Data Type	Standard	Notes for export
1.	Data exporters such as companies, public institutions, institutional associations and organizations that: • register within the China (Shanghai) Pilot	Multinational manufacturing	(1) Manufacturing management, (2) Inventory information, (3) Parts, (4) Remanufacturing, (5) Logistics supply chain	Describe each data type with inexhaustible list of typical examples.	• Require that the VIN number cannot directly or indirectly identify an individual and is not related to personal information;
		Global R&D	(1) R&D design		

	Free Trade Zone Lin-gang Special Area; • conduct cross-border data transfer; • engage in automobile manufacturing, parts and software supply, distribution, after-sales service, travel and related services.	testing	data, (2) test data, (3) R&D management data		• The video and image data involved should not cover personal information such as faces and license plates; • Inventory information and logistics supply chain data should not reflect the state's economic performance; • Unfortunately, this List does not address OTA-related data that the industry concerns a lot.
		Global after-sales service	(1) Vehicle information, (2) Fault status data, (3) Diagnostic data, (4) Customer service, (5) After-sales service records, (6) After-sales orders, (7) After-sales parts, (8) After-sales tracking, (9) After-sales reports, (10) After-sales outlets, (11) Recall management, (12) Warranty and claims		
		Global trade in used cars	(1) Vehicle information, (2) Maintenance information, (3) Insurance information		

5. Data Export Restrictions for Specific Industries

Apart from the Data Export Approvals mentioned above, some industrial regulators have issued laws and regulations related to data export controls applicable to their specific industries.

Take automotive data and industrial data as an example, the *Automotive Data Security Management Measures (for Trial Implementation)*, which came into effect on October 1, 2021, require that the Security Assessment should be conducted when transferring automotive data that falls into the scope of important data[1] out of China. It also requires that data controllers in the section should not export data beyond the

(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.

purpose, scope, method, data type and scale specified in the Security Assessment. Another example is that in February 2022, the second draft of *Data Security Management Measures in the Field of Industry and Information Technology (for Trial Implementation)* require that when it is necessary for data controllers in the field of industry and information technology to transfer important data abroad, they should conduct a Security Assessment.

Moreover, some industrial regulators have data localization requirements. This means that specific types of data cannot be transferred to and stored on overseas servers, such as population health data, mapping data, human genetic resources information.

6. Cases and penalties

Starting from 2025, regulatory authorities begin to publize cases regarding data export violations, as summarized below:

Company Name	Ilegal Behavior	Penalizing Authority	Penalty
Dior (Shanghai) Co., Ltd.	• Unauthorized Cross-Border Data Transfer: illegally transferred customer personal information to Dior's headquarters in France without first undergoing a security assessment, establishing a standard contract for personal information export, or obtaining personal information protection certification. • Lack of Informed Consent: failed to fully inform customers about how their personal information would be handled by the headquarters in France and did not obtain their specific, separate consent before transferring the data. • Inadequate Data Security: failed to implement essential security measures like encryption or de-identification for the personal information it collected.	Public security and cybersecurity authorities (Not specifically disclosed)	Not disclosed
Not disclosed	Failure to follow national regulations on cross-border data transfer security management, inadequate fulfillment of	CAC of the Yunyan District, Guiyang City, Guizhou Province	Not disclosed

	necessary security assessment and compliance review obligations, superficial and insufficient cybersecurity education, and a lack of security awareness among relevant personnel led to security risks during data transmission. Specifically, the cloud storage synchronize function was enabled on devices with public network IP addresses.		
Not disclosed	Weak cybersecurity management, including issues like weak passwords and unnecessary open ports, led to data being transferred to overseas IP addresses.	CAC of the Jingdezhen City, Jiangxi Province	Not disclosed

Penalty amount of these cases has not been disclosed yet. Pursuant to the CSL, DSL, and PIPL, the legal liabilities for violating data export regulations are as follows:

Regulation Name	**Penalty Rule**
CSL	Article 66: CIIOs who store network data or provide network data to overseas recipients in violation of regulations will face a corrective order, a warning, and confiscation of illegal gains from the relevant authorities. They may also be fined between RMB 50,000 and 500,000. Additionally, authorities can order a suspension of related operations, business closure for rectification, website shutdown, or revocation of business licenses. The directly responsible personnel will be fined between RMB 10,000 and 100,000.
DSL	Article 46: Entities that provide important data to overseas recipients in violation of regulations will receive a corrective order and a warning from the relevant authorities. They may also be fined between RMB 100,000 and 1,000,000, while directly responsible personnel can be fined between RMB 10,000 and 100,000. In severe cases, fines can range from RMB 1,000,000 to 10,000,000. Authorities may also order the suspension of related business, business closure for rectification, or revocation of business licenses. The directly responsible personnel will be fined between RMB 100,000 and 1,000,000.
PIPL	Article 66: Violating regulations by processing personal information or failing to fulfill personal information protection obligations will result in a corrective order, a warning, and confiscation of illegal gains from the department responsible for personal information protection. For applications that illegally process personal information,

	a suspension or termination of services may be ordered. If the entity refuses to make corrections, they will be fined up to RMB 1,000,000. The directly responsible personnel will be fined between RMB 10,000 and 100,000. In severe cases, the department at or above the provincial level responsible for personal information protection will issue a corrective order, confiscate illegal gains, and impose a fine of up to RMB 50,000,000 or 5% of the previous year's business turnover. They may also order a suspension of related operations, business closure for rectification, or notify relevant authorities to revoke business permits or licenses. The directly responsible personnel will be fined between RMB 100,000 and 1,000,000 and may be barred from serving as a director, supervisor, senior executive, or personal information protection officer for a certain period.

7. Compliance Advice

(1) A correct understanding of the Block Exemptions and a data exporter's judgment towards them becomes significantly important under China's current data export regulatory framework, because this determines whether the data exporter can freely export data, or must obtain one of the Data Export Approvals. Data exporters need to be very careful in applying any of the Block Exemptions. For example, many multinational companies intend to rely on Block Exemption No.2 (cross-border human resources management) to export employees' personal information. However, many fail to justify the necessity when employees' personal information must be exported. Without such justification, the Block Exemptions may not apply, and if the data exporter nonetheless relies on the Block Exemptions, it may later be deemed to have illegally exported data by the regulator and may face fines and other punishments. When in doubt as to whether the Block Exemptions apply, data exporters are advised to attempt to obtain a Data Export Approval for endorsement from regulators.

(2) Identification of sensitive personal information has become critically important under the new data export regulatory framework, because it is the triggering factor for both the Security Assessment and the SCC Filing/Certification. If Block Exemptions cannot apply, data exporters need to carefully evaluate the types of sensitive personal information they export and the amount of it, to determine whether a Security Assessment or an SCC Filing/Certification is necessary.

(3) When transferring personal information overseas, especially when it involves sensitive personal information, it is crucial to obtain the separate consent of the data subject. Separate consent means that (i) the details regarding the cross-border data transfer must be disclosed independently from the general privacy policy, (ii) and must be accompanied by a standalone checkbox for the user to actively affirm their agreement.

(4) Important data compliance cannot be neglected. Under Chinese law, important data is to be identified by the CAC or respective industrial regulators in the form of important data catalogues. Therefore, data

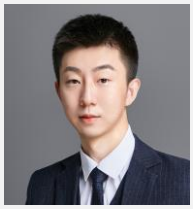
exporters are advised to closely follow the legislative trends in important data and, if catalogues relevant to their industries do come out, identify any important data they may have and need to export for the purpose of preparing for a Security Assessment.

(5) Data exporters are advised to stay abreast of the latest trends of data export inventories to take advantage of such inventories for more lenient restrictions on data export. To this end, since these inventories mostly apply to FTZs, data exporters may want to consider registering entities in FTZs or move their data processing capabilities to FTZs to become eligible for the policies.

(6) In addition to the general regulation mandated by the Data Export Approvals, data exporters shall stay aware of and carefully study the data export control measures which apply to their industries.

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

Susan Deng
+86 21 6043 3793
susan.deng@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